

Benutzerhandbuch



MoRoS UMTS PRO 2.0

Dez-09

Herausgeber:
INSYS MICROELECTRONICS GmbH
Waffnergasse 8
93047 Regensburg, Deutschland
Telefon: +49 (0)941/56 00 61
Telefax: +49 (0)941/56 34 71
E-Mail: insys@insys-tec.de
Internet: http://www.insys-tec.de

Stand: Dez-09
Artikelnummer: 31-22-03.148
Version: 1.2
Sprache: DE

1 Sicherheit

Gefahr!



Nässe und Flüssigkeiten aus der Umgebung können ins Innere des Gerätes gelangen.

Lebensgefahr durch Stromschlag bei Berührung!

Der MoRoS UMTS PRO 2.0 darf nicht in nassen oder feuchten Umgebungen oder direkt in der Nähe von Gewässern eingesetzt werden. Installieren Sie das Gerät an einem trockenen, vor Spritzwasser geschützten Ort. Schalten Sie die Spannung ab, bevor Sie Arbeiten an einem Gerät durchführen, das mit Feuchtigkeit in Berührung kam.

Gefahr!



Überspannung.

Brandgefahr!

Sichern Sie den MoRoS UMTS PRO 2.0 mit einer geeigneten Sicherung gegen Überspannung ab.

Gefahr!



Überstrom.

Brandgefahr!

Sichern Sie den MoRoS UMTS PRO 2.0 mit einer geeigneten Sicherung gegen Ströme höher als 1,6 A ab.

Warnung!



Kurzschlüsse und Beschädigung durch unsachgemäße Reparaturen und Öffnen von Wartungsbereichen.

Feuer, Funktionsausfall und Verletzungsgefahr!

Nur Personen, deren Ausbildung oder Kenntnisstand dem Berufsbild des „Elektronikers für Betriebstechnik“ entspricht, dürfen den MoRoS UMTS PRO 2.0 öffnen und Reparaturarbeiten daran ausführen.

Hinweis



Beschädigung des Gerätes durch Überspannung!

Spannungsspitzen aus dem Stromnetz können den MoRoS UMTS PRO 2.0 beschädigen.

Installieren Sie einen geeigneten Überspannungsschutz.

Hinweis



Beschädigung durch Chemikalien!

Ketone und chlorierte Kohlenwasserstoffe lösen den Kunststoff des Gehäuses und beschädigen die Oberfläche des Geräts.

Bringen Sie das Gerät auf keinen Fall mit Ketonen (z.B. Aceton) und chlorierten Kohlenwasserstoffen (z.B. Dichlormethan) in Berührung.

Hinweis



Abstand von Antennen zu Personen!

Ein zu geringer Abstand von GSM-Antennen zu Personen kann die Gesundheit beeinträchtigen.

Bitte beachten Sie, dass die GSM-Antenne während des Betriebs mindestens 20 cm von Personen entfernt sein muss.

Hinweis



Exportbeschränkung für FCC!

Mögliches Vergehen gegen Zulassungsbestimmungen.

Wenn das Endprodukt nicht für eine Verwendung im Gebiet der Vereinigten Staaten zugelassen ist, hat der Applikationshersteller sicherzustellen, dass die Frequenzbänder 850 MHz und 190 MHz deaktiviert und die Bandeinstellungen dem Endanwender nicht zugänglich sind. Wenn diese Anforderungen nicht erfüllt werden (z.B. weil die AT-Befehls-Schnittstelle dem Endanwender zugänglich ist), liegt es in der Verantwortung des Applikationsherstellers, jederzeit sicherzustellen, dass die Anwendung nicht in Länder im Gültigkeitsbereich der FCC exportiert wird.

2 Lieferumfang

Der Lieferumfang für den MoRoS UMTS PRO 2.0 umfasst die im Folgenden aufgeführten Zubehörteile. Bitte kontrollieren Sie, ob alle angegebenen Zubehörteile in Ihrem Karton enthalten sind. Sollte ein Teil fehlen oder beschädigt sein, so wenden Sie sich bitte an Ihren Distributor.

- 1 MoRoS UMTS PRO 2.0
- 1 Quick Installation Guide
- 1 Service-CD mit Benutzerhandbuch im PDF-Format

Optionales Zubehör ist nicht im Lieferumfang des MoRoS UMTS PRO 2.0 enthalten. Folgende Teile sind bei Ihrem Distributor oder bei INSYS MICROELECTRONICS erhältlich:

- GSM-Antenne mit Magnetfuß

3 Bestimmungsgemäße Verwendung

Das Gerät „MoRoS UMTS PRO 2.0“ dient ausschließlich zu den aus der Funktionsübersicht hervorgehenden Einsatzzwecken. Zusätzlich darf das Gerät für die folgenden Zwecke eingesetzt werden:

- Einsatz & Montage in einem industriellen Schaltschrank
- Übernahme von Schalt- sowie Datenübertragungsfunktionen in Maschinen, die der Maschinenrichtlinie 2006/42/EG entsprechen
- Einsatz als Datenübertragungsgerät an einer speicherprogrammierbaren Steuerung

Das Gerät „MoRoS UMTS PRO 2.0“ darf **nicht** zu den folgenden Zwecken und unter diesen Bedingungen verwendet oder betrieben werden:

- Steuerung oder Schaltung von Maschinen und Anlagen, die nicht der Richtlinie 2006/42/EG entsprechen
- Einsatz, Steuerung, Schaltung und Datenübertragung in Maschinen oder Anlagen, die in explosionsfähigen Atmosphären betrieben werden
- Steuerung, Schaltung und Datenübertragung von Maschinen, deren Funktionen oder deren Funktionsausfall eine Gefahr für Leib und Leben darstellen können

4 Technische Daten

4.1 Physikalische Merkmale

Gefahr!



Überspannung.

Brandgefahr!

Sichern Sie den MoRoS UMTS PRO 2.0 mit einer geeigneten Sicherung gegen Überspannung ab.

Die angegebenen Daten wurden bei nominaler Eingangsspannung, unter Volllast und einer Umgebungstemperatur von 25°C gemessen. Die Grenzwerttoleranzen unterliegen den üblichen Schwankungen.

Physikalische Eigenschaft	Wert
Betriebsspannung	minimal 10 V DC maximal 60 V DC
Leistungsaufnahme Ruhe	ca. 3 W
Leistungsaufnahme Verbindung	ca. 6,5 W
Pegel Eingänge	HIGH-Pegel = 3-12 V (Kontakt offen bzw. Spannungsfestigkeit bei Fremdspeisung) LOW-Pegel =0-1 V
Stromaufnahme eines aktiven Eingangs gegen GND (intern 3,3 V)	Typisch 0,5 mA (bei Aktivierung des Eingangs durch verbinden mit GND)
Schaltausgang, max. Schaltspannung	30 V (DC) / 42 V (AC)
Schaltausgang, max. Strombelastung	1 A (DC) / 0,5 A (AC)
Abgestrahlte Leistung: UMTS 850: Class 3 UMTS 1900: Class 3 UMTS 2100: Class 3 EGSM 850 und 900: Class 4 GSM 1800 und 1900: Class 1 EGSM 850 und 900: Class E2 GSM 1800 und 1900: Class E2	 0,25 W 0,25 W 0,25 W 2 W 1 W 0,5 W 0,5 W
Gewicht	350 g
Abmessungen (Breite x Tiefe x Höhe)	70 mm x 110 mm x 75 mm
Temperaturbereich	-20° C – 55° C
Maximale zulässige Luftfeuchtigkeit	95% nicht kondensierend

Physikalische Eigenschaft	Wert
Schutzart	Gehäuse IP40, Schraubklemmen IP20

Tabelle 1: Physikalische Eigenschaften

4.2 Technologische Merkmale

Technologische Eigenschaft:	Beschreibung
GSM-Frequenzen (2G)	850, 900, 1800, 1900 MHz; Die Frequenz-Bänder 850 Mhz und 1900 Mhz sind wegen FCC-Bestimmungen deaktiviert. Um die Frequenz-Bänder zu aktivieren, kontaktieren Sie bitte den INSYS Support.
UMTS-Frequenzen (3G)	850, 1900, 2100 MHz; Das Frequenz-Band 850 Mhz ist wegen FCC-Bestimmungen deaktiviert. Um das Frequenz-Band zu aktivieren, kontaktieren Sie bitte den INSYS Support.
SIM-Kartenleser	Unterstützung für 1,8 V- und 3,3 V-SIM-Karten
SMS	SMS-Versand, eingehende SMS können empfangen werden, sind aber nicht über das Web-Interface zugänglich.
CSD	bis 14,4 kBit/s
GPRS	GPRS Multislot Class 12, Coding scheme 1 bis 4, PBCCH, Mobile Station Class B
EDGE (EGPRS)	EDGE Multislot Class 10, Modulation and Coding Scheme MCS 1-9
UMTS	Uplink bis 384 kBit/s / Downlink bis 384 kBit/s HSDPA nach UE CAT. [1-6]. 11. 12 Compressed mode (3GPP TS25.212) Downlink bis 3,6 MBit/s

Tabelle 2: Technologische Merkmale

5 Anzeigen- und Bedienelemente

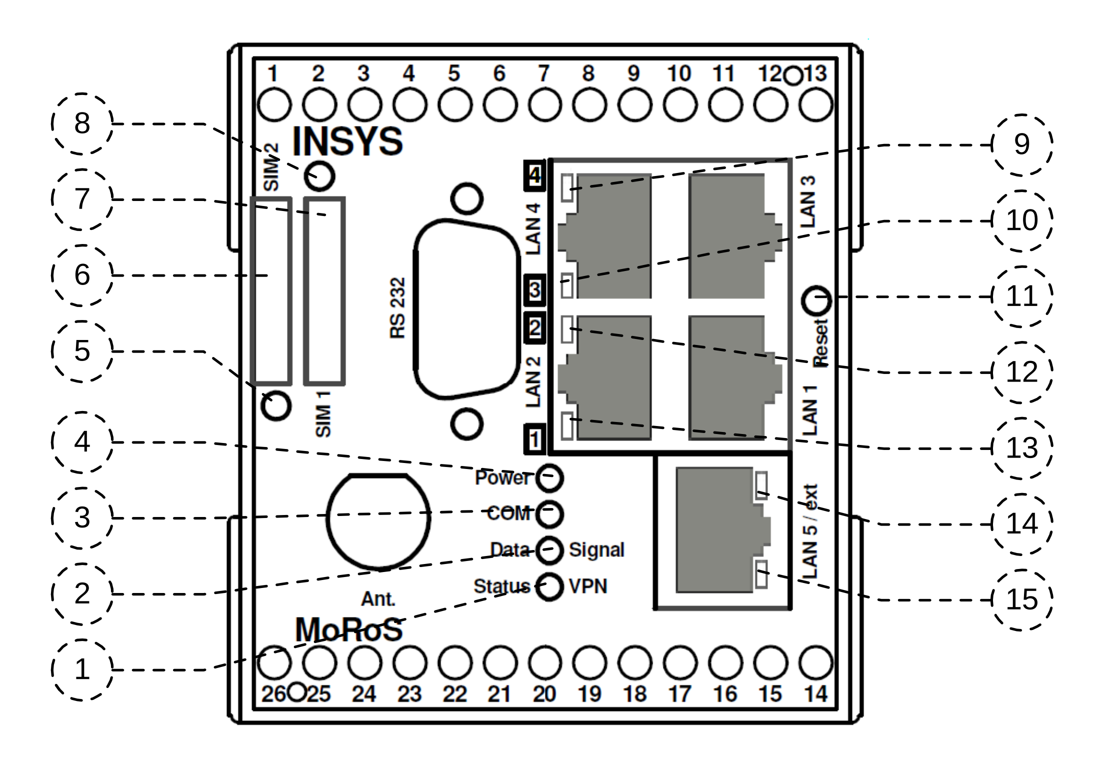


Abbildung 1: LEDs auf der Gerätvorderseite

Position	Bezeichnung
1	Status/VPN LED
2	Data/Signal LED
3	COM LED
4	Power LED
5	SIM-Karte 2 - Auswurfknopf
6	SIM-Karte 2 - Kartenhalter
7	SIM-Karte 1 - Kartenhalter
8	SIM-Karte 1 - Auswurfknopf
9	Status LED für Switch LAN 4
10	Status LED für Switch LAN 3
11	Reset-Taster
12	Status LED für Switch LAN 2
13	Status LED für Switch LAN 1
14	Status LED für Switch LAN 5 / ext.
15	Status LED für Switch LAN 5 / ext.

Tabelle 3: Beschreibung der LEDs auf der Gerätevorderseite

5.1 Bedeutung der Anzeigen

LED	Farbe	Funktion	aus	blitzt	blinkt	an
Switch LAN 1-4	gelb	Link 10 MBit/s			Datenverkehr	verbunden
	grün	Link 100 MBit/s				
Switch LAN 5	orange	Link 10 MBit/s			Datenverkehr	verbunden
	grün	Link 100 MBit/s				
Power	grün	Versorgung	fehlt			vorhanden
COM	grün	Connect	offline			aufgebaut
	orange	PPP-Link				
Data / Signal	grün	SIM-Karte 1	kein Signal o. ausgebucht	PPP-Datenverkehr	Feldstärke (siehe Tabelle 5)	
	orange	SIM-Karte 2				
Status / VPN	grün	VPN				Client oder Server aufgebaut
	rot	Status				Initialisierung, FW-Update, Störung

Tabelle 4: Bedeutung der LED-Anzeigen

Blinktakt LED Signal	Wertigkeit	Qualität des Signals
900 ms an, 100 ms aus	20 .. 32	sehr gut
200 ms an, 200 ms aus	13 .. 19	gut
100 ms an, 900 ms aus	0 .. 12	schlecht
aus	99 (nicht feststellbar)	ungenügend

Tabelle 5: Blinkcode der Data/Signal LED

5.2 Funktion der Bedienelemente

Bezeichnung	Bedienung	Bedeutung
Reset-Taster	Einmal kurz drücken.	Setzt MoRoS UMTS PRO 2.0 per Software zurück und startet neu. (Soft Reset)
	Mindestens 3 Sekunden lang drücken.	Setzt die Hardware des MoRoS UMTS PRO 2.0 zurück und startet neu. (Hard Reset)
	Innerhalb von 2 Sekunden dreimal hintereinander kurz drücken.	Löscht alle Einstellungen des MoRoS UMTS PRO 2.0 und setzt das Gerät auf Werkseinstellungen zurück
SIM-Karten-Auswurfknopf	Drücken mit spitzem Gegenstand	Wirft den SIM-Kartenhalter aus.

Tabelle 6: Funktionsbeschreibung und Bedeutung der Bedienelemente

6 Anschlüsse

6.1 Anschlüsse Vorderseite

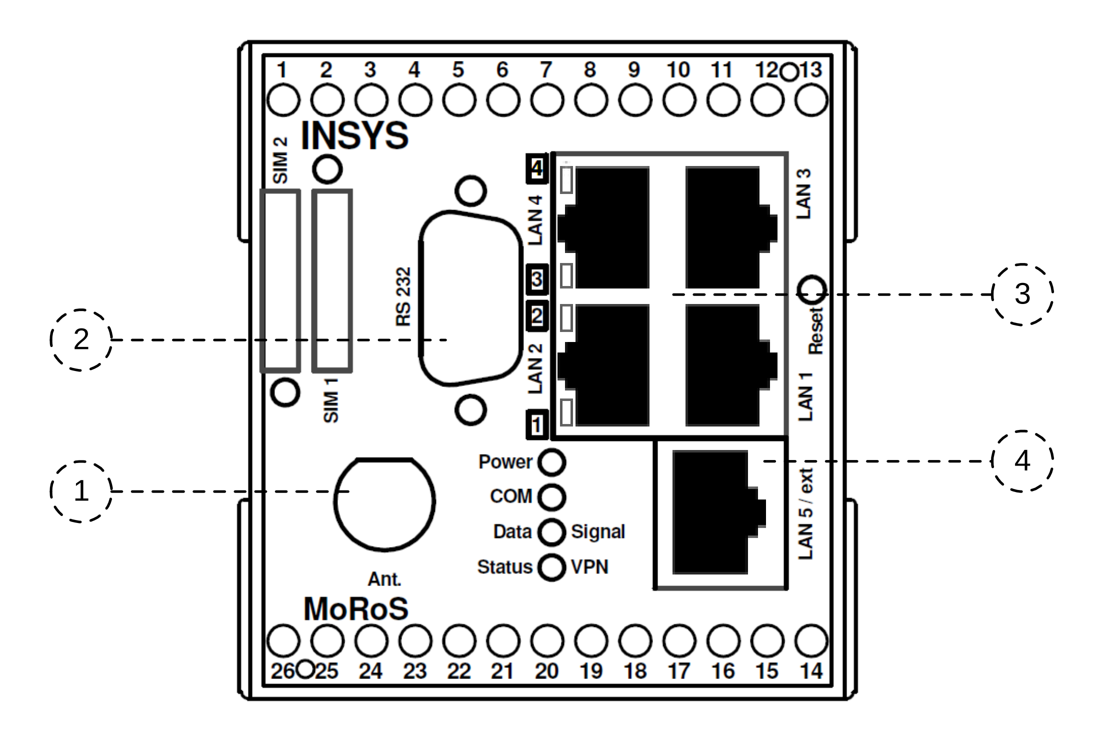


Abbildung 2: Anschlüsse auf der Gerätevorderseite

Position	Bezeichnung
1	GSM-Antennenanschluss (FME-Buchse)
2	Serielle Schnittstelle (RS232-Buchse V.24/V.28)
3	Switch mit 4 Ethernet-Ports (RJ45, 10/100 BT)
4	Ethernet-Port (RJ45, 10/100 BT)

Tabelle 7: Beschreibung der Anschlüsse auf der Gerätevorderseite

6.2 Klemmanschlüsse Oberseite

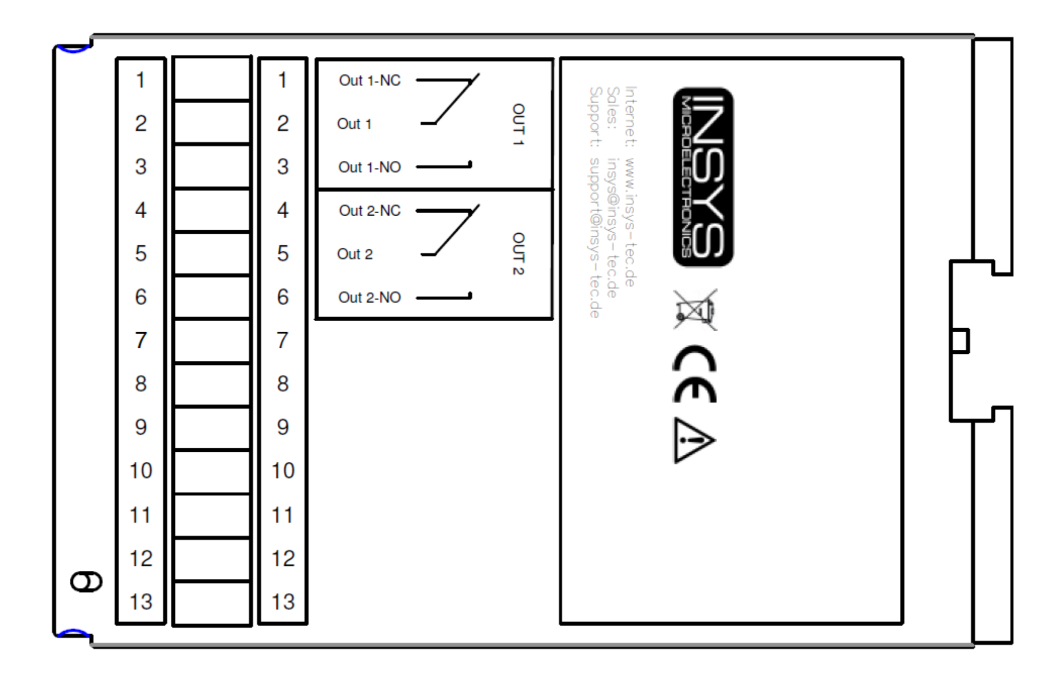


Abbildung 3: Anschlüsse auf der Geräteoberseite

Klemme	Bezeichnung	Beschreibung
1	OUT 1-NC	Ausgang1 Ruhekontakt
2	OUT 1	Ausgang1
3	OUT 1-NO	Ausgang1 Arbeitskontakt
4	OUT 2-NC	Ausgang2 Ruhekontakt
5	OUT 2	Ausgang2
6	OUT 2-NO	Ausgang2 Arbeitskontakt

Tabelle 8: Beschreibung der Anschlüsse auf der Geräteoberseite

6.3 Klemmanschlüsse Unterseite

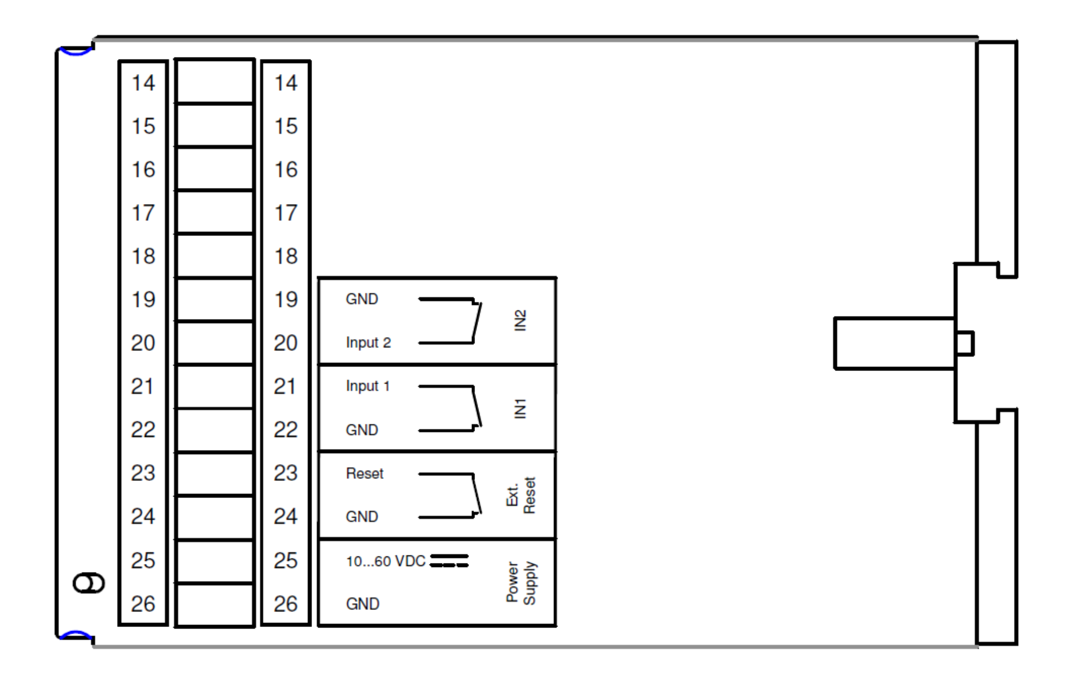


Abbildung 4: Anschlüsse auf der Geräteunterseite

Klemme	Bezeichnung	Beschreibung
19	GND	Ground (Masse)
20	Input 2	Eingang 2
21	Input 1	Eingang 1
22	GND	Ground (Masse)
23	Reset	Reset-Eingang
24	GND	Ground (Masse)
25	10 ... 60 VDC	Spannungsversorgung 10 V – 60 V DC
26	GND	Ground (Masse)

Tabelle 9: Beschreibung der Anschlüsse auf der Geräteunterseite

6.4 Anschlussbelegung der seriellen Schnittstelle

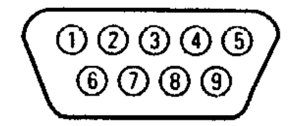


Abbildung 5: 9-polige Sub-D Buchse am Gerät

Pin	Belegung	Beschreibung
1	DCD	Data Carrier Detect
2	RXD	Receive Data
3	TXD	Transmit Data
4	DTR	Data Terminal Ready
5	GND	Ground
6	DSR	Data Set Ready
7	RTS	Request To Send
8	CTS	Clear To Send
9	RI	Ring Indication

Tabelle 10: Beschreibung der Pin-Belegung der Sub-D Buchse

7 Funktionsübersicht

Der MoRoS UMTS PRO 2.0 bietet Ihnen die folgenden Funktionen:

- **Konfiguration über Weboberfläche**

  Alle Funktionen des MoRoS UMTS PRO 2.0 können über eine Weboberfläche konfiguriert und eingestellt werden. Der Zugriff auf die Weboberfläche ist mit einer Benutzername- und Passwortabfrage geschützt. Der TCP Port, unter dem die Weboberfläche erreichbar ist, kann frei eingestellt werden.

- **Seriell-Ethernet-Gateway**

  Der MoRoS UMTS PRO 2.0 kann auf einem bestimmten Netzwerkport ankommende Daten auf der seriellen Schnittstelle ausgeben. Ebenso werden an der seriellen Schnittstelle ankommende Daten an eine IP-Gegenstelle versendet. Das Seriell-Ethernet-Gateway erlaubt zusammen mit dem IN-SYS VCOM-Treiber die transparente Übertragung einer seriellen Verbindung über ein Netzwerk.

- **NAT und Portforwarding**

  Der MoRoS UMTS PRO 2.0 ist ein Router, der Datenpakete auch durch NAT und Portforwarding weiterleiten kann. Nach festlegbaren Regeln leitet MoRoS UMTS PRO 2.0 eingehende IP-Pakete an definierbare Ports und Portbereiche zu IP-Adressen und Ports im LAN weiter.

- **Einwahl-PPP-Server (Dial-In)**

  Der MoRoS UMTS PRO 2.0 kann als PPP-Einwahlserver verwendet werden. Wie bei einem Internetprovider kann ein Anrufer eine PPP-Verbindung zum MoRoS UMTS PRO 2.0 aufbauen, um auf das dahinterliegende Netzwerk zuzugreifen.

- **Aufbau einer PPP-Verbindung durch eingehenden Anruf (Callback)**

  Der MoRoS UMTS PRO 2.0 identifiziert Anrufer und baut automatisch eine PPP-Verbindung zu einer zuvor bestimmten Gegenstelle (z.B. einem Interprovider) auf. Dabei kann sich der Anrufer, der den Verbindungsaufbau auslöst, über eine PPP-Authentifizierungsmethode identifizieren.

- **Aufbau einer PPP-Verbindung über einen Digitaleingang**

  Der MoRoS UMTS PRO 2.0 baut nach Auslösung durch einen Digitaleingang eine PPP-Verbindung zu einer zuvor bestimmten Gegenstelle (z.B. einem Interprovider) auf. Es ist auch möglich, diese Verbindung nur so lange aufrecht zu erhalten, wie das Signal anliegt.

- **Automatische Anwahl einer PPP-Gegenstelle (Dial-Out)**

  Der MoRoS UMTS PRO 2.0 baut eine Verbindung zu einer PPP-Gegenstelle (z.B. Internetprovider) auf, sobald er ausgehenden Netzwerkverkehr registriert.

- **Wählfilter für das Auslösen eines Verbindungaufbaus**

  Über Regeln können Sie festgelegen, welcher Netzwerkverkehr oder Netzwerkteilnehmer einen Verbindungsaufbau auslösen darf.

- **PPP-Standleitungsbetrieb**

  Der MoRoS UMTS PRO 2.0 kann eine dauerhafte Verbindung über eine „Wählleitung“ herstellen und aufrecht erhalten. So ist es möglich, mit einem Netzwerk über eine Wählverbindung wie über eine „Standleitung“ zu kommunizieren.

- **Periodischer PPP-Verbindungsaufbau**

  MoRoS UMTS PRO 2.0 kann zeitgesteuert eine PPP-Verbindung aufbauen ebenso zeitgesteuert schließen. Für den Verbindungsaufbau und den Verbindungsabbau können feste Uhrzeiten eingestellt werden.

- **OpenVPN-Server**

  Der MoRoS UMTS PRO 2.0 kann als OpenVPN-Server fungieren. So können Maschinen von außen über unsichere Netzwerke eine sichere Verbindung zum LAN hinter dem MoRoS UMTS PRO 2.0 herstellen. Voraussetzung dafür ist, dass das Gerät über eine paketbasierte Verbindung erreichbar ist (öffentliche IP-Adresse) oder dass ständig eine CSD-Verbindung besteht.

- **OpenVPN-Client**

  Der MoRoS UMTS PRO 2.0 kann auch ein ganzes LAN über eine unsichere Internet-Verbindung abhör- und störungssicher durch einen VPN-Tunnel mit einem anderen Netzwerk (z.B. dem Firmennetzwerk) verbinden. Der MoRoS UMTS PRO 2.0 kann sich dafür als Client zu einem OpenVPN-Server verbinden.

- **Verschiedene Methoden der VPN-Authentifizierung**

  Der MoRoS UMTS PRO 2.0 unterstützt die Authentifizierung bei Verbindung zu einem OpenVPN-Server über einen statischen Schlüssel, über ein Zertifikat mit Benutzernamen und Passwort oder über ein Zertifikat alleine. Weiterhin kann der MoRoS UMTS PRO 2.0 auch eine OpenVPN-Verbindung ohne Authentifizierung aufbauen.

- **Firewall (Statefull Firewall)**

  Die MoRoS UMTS PRO 2.0-Firewall ermöglicht es, ein- und ausgehende IP-Verbindungen zu beschränken. Für jede Verbindung und für jeden gespeicherten Benutzer kann eine flexible Regel angelegt werden. Entspricht eine Verbindung durch den MoRoS UMTS PRO 2.0 einer dieser Firewall-Regeln, so wird die Verbindung zugelassen, andernfalls wird die Verbindung unterbunden. So kann die Sicherheit durch unerwünschte Zugriffe auf das Netzwerk hinter dem MoRoS UMTS PRO 2.0 erhöht werden. „Statefull Firewall“ bedeutet, dass der MoRoS UMTS PRO 2.0 automatisch die Firewall für Datenverkehr anpasst, der von erlaubten Datenpaketen initiiert wurde. Dies erlaubt Verbindungen auch für Protokolle mit speziellen Anforderungen, z.B. FTP.

- **Konfigurierbarer Ethernet-Switch**

  Für jeden Port am Switch des MoRoS UMTS PRO 2.0 kann die Übertragungsrate, der Übertragungsmodus und die LED-Anzeige für bestimmte Netzwerkereignisse einzeln eingestellt werden. In der Werkseinstellung erkennt der MoRoS UMTS PRO 2.0 die Einstellungen automatisch.

- **Portspiegelung am Ethernet-Switch für Analysezwecke**

  Ein Port am Switch des MoRoS UMTS PRO 2.0 kann eine Kopie der Daten an einem anderen Netzwerkport des Switchs wiedergeben. An diesem Mirror-Port können die übertragenen Daten für Analysezwecke (z.B. für Intrusion Detection Systeme, Problemanalyse von Endgeräten) gelesen werden, ohne dass der Netzwerkverkehr beeinflusst wird.

- **SMS-Versand über Impulse am Schalteingang**

  11 SMS-Nachrichten mit individuellem Text und Empfänger können durch Impulse am Eingang 1 versendet werden.

- **Digitale Schaltausgänge und Eingänge**

  Der MoRoS UMTS PRO 2.0 verfügt über zwei potentialfreie Schaltausgänge, die zum Schalten weiterer Funktionen in einer Applikation genutzt werden können. Der MoRoS UMTS PRO 2.0 besitzt ebenfalls digitale Eingänge, die zum Aufbau von Verbindungen oder zum Versand von Meldungen via SMS genutzt werden können.

- **Zeitsynchronisation über NTP**

  Der MoRoS UMTS PRO 2.0 kann seine Systemzeit über das Network Time Protocol mit einem NTP-Server im Internet synchronisieren. So ist die Systemzeit immer aktuell und die interne Uhr muss nicht manuell eingestellt werden. Zusätzlich kann die Zeit und das Datum manuell eingestellt werden, wenn kein NTP-Server erreichbar ist.

- **HTTP und HTTPS Proxy mit URL-Filter**

  Der Proxy dient dazu, um den Zugriff auf Webadressen für Applikationen im lokalen Netz des MoRoS UMTS PRO 2.0 zu beschränken sowie um Verbindungs-Timeouts zu vermeiden. Der MoRoS UMTS PRO 2.0 unterstützt die Protokolle HTTP und HTTPS. Der Proxy des MoRoS UMTS PRO 2.0 hält Verbindungen während dem Verbindungsaufbaus des Kommunikationsgerätes geöffnet, um einem vorzeitigen Timeout vorzubeugen. Der Proxy arbeitet nicht als Cache für häufig aufgerufene Webseiten.

- **Log-Dateien**

  Die Systemmeldungen des MoRoS UMTS PRO 2.0 können als Textdateien über die Weboberfläche heruntergeladen werden.

- **Herunterladbare Konfigurationsdateien**

  Die Konfiguration des MoRoS UMTS PRO 2.0 kann als Datei heruntergeladen werden. Die Datei kann als Sicherheitskopie zur Konfiguration des MoRoS UMTS PRO 2.0 nach einem Werksreset verwendet werden oder zum bequemen Laden einer gleichen Konfiguration in verschiedene MoRoS UMTS PRO 2.0.

- **Firmware-Update über Weboberfläche**

  Die Firmware des MoRoS UMTS PRO 2.0 kann über die Weboberfläche aktualisiert werden. Ein Update kann lokal oder aus der Ferne durchgeführt werden.

- **Optionales redundantes Kommunikationsgerät anschließbar.**

  Sie können ein zweites INSYS Kommunikationsgerät über die serielle Schnittstelle an den MoRoS UMTS PRO 2.0 anschließen, um dadurch die Dial-Out- und Dial-In- Kommunikation durch Redundanz abzusichern und die Verfügbarkeit zu erhöhen.

8 Symbole und Formatierungen dieser Anleitung

Im Folgenden werden die Festlegungen, Formatierungen und Symbole erklärt, die in diesem Handbuch verwendet werden. Die unterschiedlichen Symbole sollen Ihnen das Lesen und Auffinden der für Sie wichtigen Information erleichtern. Der folgende Text entspricht in seiner Struktur den Handlungsanweisungen dieses Handbuchs.

Fett gedruckt: Das Handlungsziel. Hier erfahren Sie, was Sie mit den folgenden Schritten erreichen

Nach der Nennung des Handlungsziels wird detaillierter erklärt, was mit der Handlungsanweisung erreicht werden soll. So können Sie entscheiden, ob der Abschnitt überhaupt für Sie relevant ist.

⇢ Vorbedingungen, die erfüllt sein müssen, damit die nachfolgenden Schritte sinnvoll abgearbeitet werden können, sind mit einem Pfeil gekennzeichnet. Hier erfahren Sie zum Beispiel, welche Software oder welches Zubehör Sie benötigen.

1. ***Ein einzelner Handlungsschritt: Dieser sagt Ihnen, was Sie an dieser Stelle tun müssen. Zur besseren Orientierung sind die Schritte nummeriert.***

✓ Ein Ergebnis, das Sie nach Ausführen eines Schrittes bekommen, ist mit einem Häkchen gekennzeichnet. Hier können Sie kontrollieren, ob die zuvor gemachten Schritte erfolgreich waren.

ⓘ Zusätzliche Informationen, die an dieser Stelle Ihre Beachtung finden sollten, sind mit einem eingekreisten „i“ gekennzeichnet. Hier werden Sie auf mögliche Fehlerquellen und deren Vermeidung hingewiesen.

➢ *Alternative Ergebnisse und Handlungsschritte sind mit einem Pfeil gekennzeichnet. Hier erfahren Sie, wie Sie auf einem anderen Weg zum gleichen Ergebnis kommen, oder was Sie tun können, falls Sie an dieser Stelle nicht das erwartete Ergebnis bekommen haben.*

9 Montage

Dieses Kapitel erklärt, wie Sie den MoRoS UMTS PRO 2.0 auf einer Hutschiene montieren, die Stromversorgung anklemmen und wie Sie ihn wieder demontieren können.

Gefahr!



Offen liegende elektrische Komponenten!

Lebensgefahr durch Stromschlag!

Vor der Montage die Stromversorgung des Schaltschranks abschalten und gegen Wiedereinschalten sichern.

Gefahr!



Nässe und Flüssigkeiten aus der Umgebung können ins Innere des MoRoS UMTS PRO 2.0 gelangen.

Lebensgefahr durch Stromschlag bei Berührung!

Der MoRoS UMTS PRO 2.0 darf nicht in nassen oder feuchten Umgebungen oder in der direkten Nähe von Gewässern eingesetzt werden. Installieren Sie das Gerät an einem trockenen, vor Spritzwasser geschützten Ort. Schalten Sie den Strom ab, bevor Sie Arbeiten an einem Gerät durchführen, das mit Feuchtigkeit in Berührung kam.

Hinweis



Gerätezerstörung durch falsche Spannungsquelle!

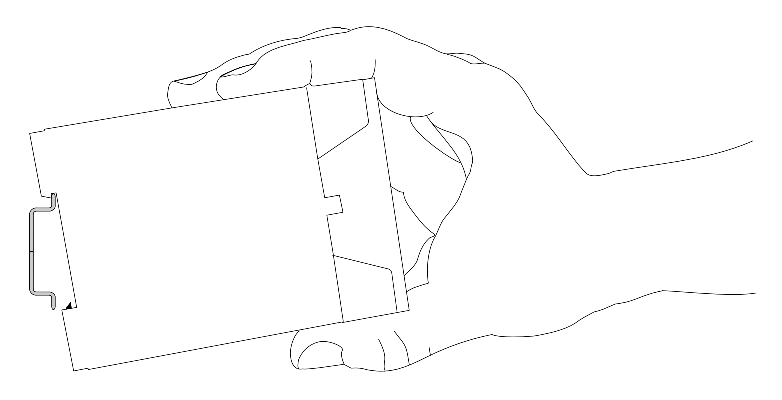
Wenn der MoRoS UMTS PRO 2.0 mit einer Spannungsquelle betrieben wird, die eine größere Spannung als die zulässige Betriebspannung des MoRoS UMTS PRO 2.0 liefert, wird das Gerät zerstört.

Sorgen Sie für eine geeignete Spannungsversorgung. Den richtigen Spannungsbereich für den MoRoS UMTS PRO 2.0 finden Sie im Kapitel „Technische Daten“.

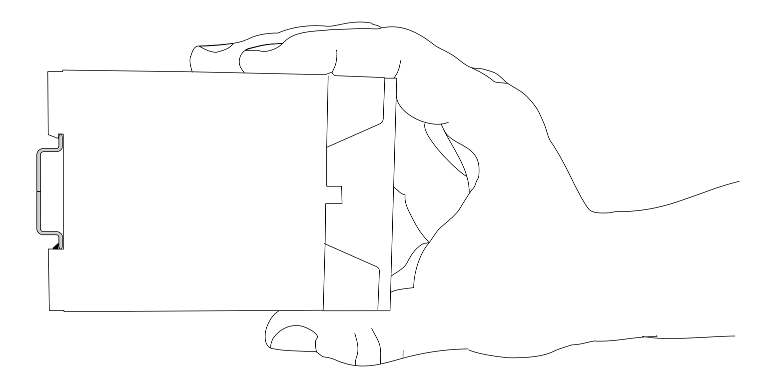
Gerät auf Hutschiene montieren

So montieren Sie den MoRoS UMTS PRO 2.0 auf einer DIN-Hutschiene:

1. ***Setzen Sie das Gerät, wie in der folgenden Abbildung gezeigt, an der Hutschiene an. An der oberen und der unteren Außenkante der Hutschienennut am MoRoS UMTS PRO 2.0 befinden sich jeweils zwei Rasthaken.***
Haken Sie die oberen beim Ansetzen hinter der Oberkante der Hutschiene ein.



2. ***Klappen Sie den MoRoS UMTS PRO 2.0 senkrecht zur Hutschiene, bis die zwei unteren, beweglichen Rasthaken in der Hutschiene einrasten.***



✓ Der MoRoS UMTS PRO 2.0 ist nun fertig montiert.

Stromversorgung anklemmen

⇢ Das Gerät ist bereits auf der Hutschiene montiert.

⇢ Die Spannungsversorgung steht bereit und ist abgeschaltet.

1. ***Klemmen Sie das Massekabel der Spannungsversorgung an der Klemme „GND“ an.***

2. ***Klemmen Sie den Pluspol der Spannungsversorgung an der Klemme für die Spannungsversorgung an.***

Gerät von Hutschiene demontieren

So demontieren Sie den MoRoS UMTS PRO 2.0 von einer Hutschiene in einem Schaltschrank:

⇢ Sie benötigen einen Schlitzschraubendreher mit 4,5 mm Klingenbreite.

⇢ Die Stromversorgung des Schaltschranks ist abgestellt und gegen versehentliches Wiedereinschalten gesichert.

⇢ Alle Kabel am MoRoS UMTS PRO 2.0 sind abgeklemmt.

Gefahr

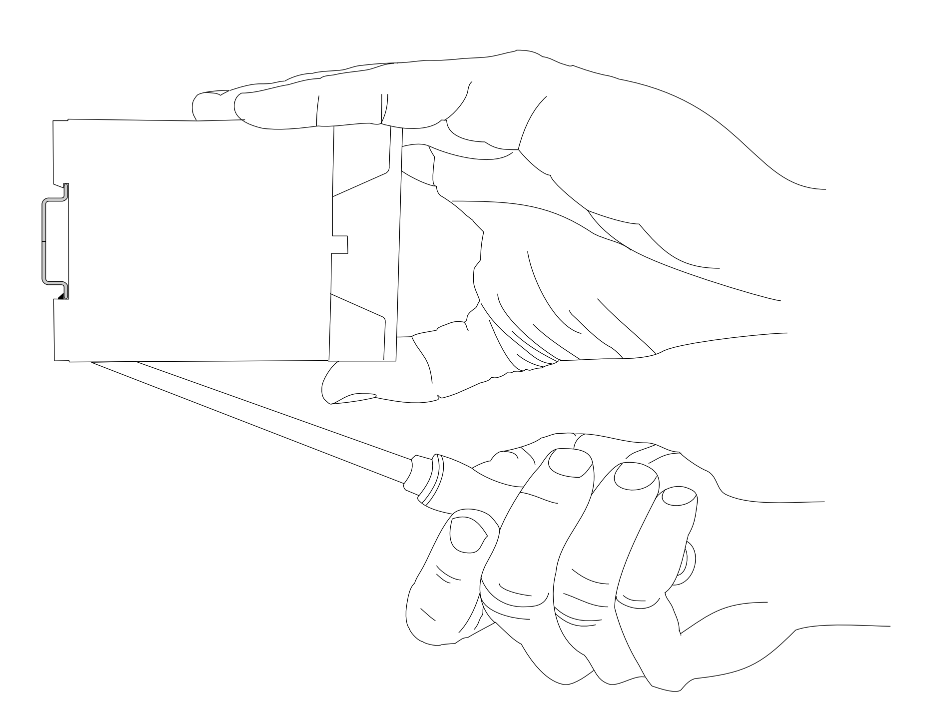


Offen liegende elektrische Komponenten!

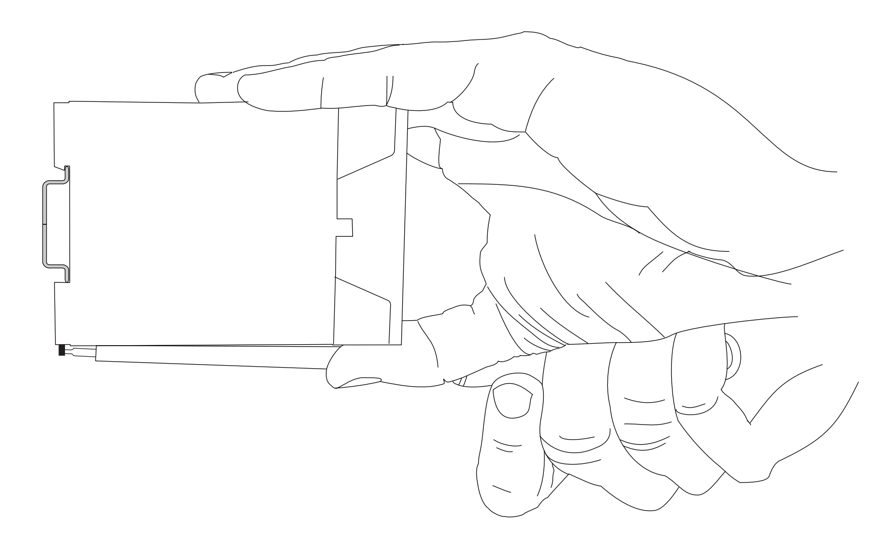
Lebensgefahr durch Stromschlag!

Vor der Demontage Stromversorgung abschalten und gegen Wiedereinschalten sichern.

1. Führen Sie den Schlitz-Schraubendreher wie in der folgenden Abbildung gezeigt in die Rille hinten im Boden des MoRoS UMTS PRO 2.0 ein.



2. Bewegen Sie den Schlitzschraubendreher wie in der folgenden Abbildung gezeigt zum MoRoS UMTS PRO 2.0 hin.



✓ Die Kunststofffeder mit den unteren Rasthaken wird auseinandergezogen.

3. Während Sie die Kunststofffeder des Rasthakens gespannt halten, klappen Sie den MoRoS UMTS PRO 2.0 von der Hutschiene weg.

4. Haken Sie den MoRoS UMTS PRO 2.0 aus und nehmen Sie ihn senkrecht zur Hutschiene ab.

10 Inbetriebnahme

Dieses Kapitel erklärt, wie Sie den MoRoS UMTS PRO 2.0 in Betrieb nehmen; d. h. den MoRoS UMTS PRO 2.0 mit einem PC verbinden und zur Konfiguration vorbereiten.

SIM-Karte in den MoRoS UMTS PRO 2.0 einsetzen.

So setzen Sie die SIM-Karte in den MoRoS UMTS PRO 2.0 ein.

⇢ Die Stromversorgung des MoRoS UMTS PRO 2.0 ist abgestellt.

⇢ Sie benötigen eine funktionierende SIM-Karte Ihres Mobilfunkproviders.

⇢ Sie benötigen die dazugehörige PIN.

⇢ Sie benötigen einen spitzen Gegenstand zum Betätigen des SIM-Karten-Auswurfknopfs, z.B. einen Schraubendreher mit maximal 1.5mm Klingenbreite.

1. ***Drücken Sie mit dem spitzen Gegenstand den SIM-Karten-Auswurfknopf von SIM-Karte 1.***

ⓘ Wenn nur eine SIM-Karte verwendet wird, muss diese immer in den Kartenhalter für die SIM-Karte 1 eingelegt werden!

✓ Der SIM-Kartenhalter wird ein Stück weit aus dem Gehäuse geschoben.

2. ***Entnehmen Sie den SIM-Kartenhalter.***

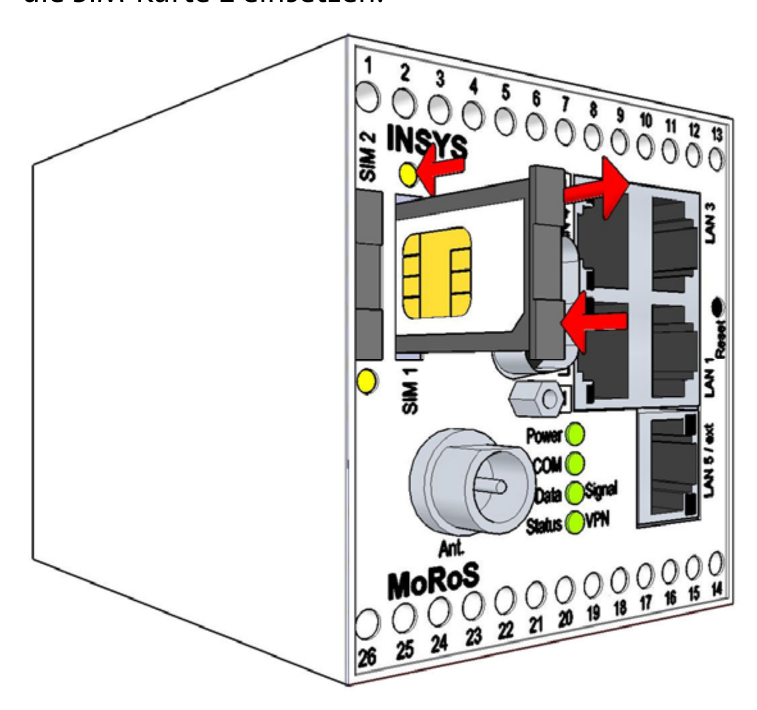
3. ***Setzen Sie Ihre SIM-Karte in den Halter ein.***

ⓘ Die SIM-Karte passt nur in einer Position korrekt in den SIM-Kartenhalter. Achten Sie darauf, dass die SIM-Karte nicht über den Halter hinaus ragt.

4. ***Setzen Sie den SIM-Kartenhalter zusammen mit der SIM-Karte, die Kontakte der SIM-Karte zur linken (für SIM-Karte 1) Gehäusewand zeigend, wieder in den MoRoS UMTS PRO 2.0 ein.***

5. ***Drücken Sie mit dem Finger den SIM-Kartenhalter mit der eingesetzten SIM-Karte mit einem Finger vorsichtig in das Gehäuse, bis der Halter einrastet.***

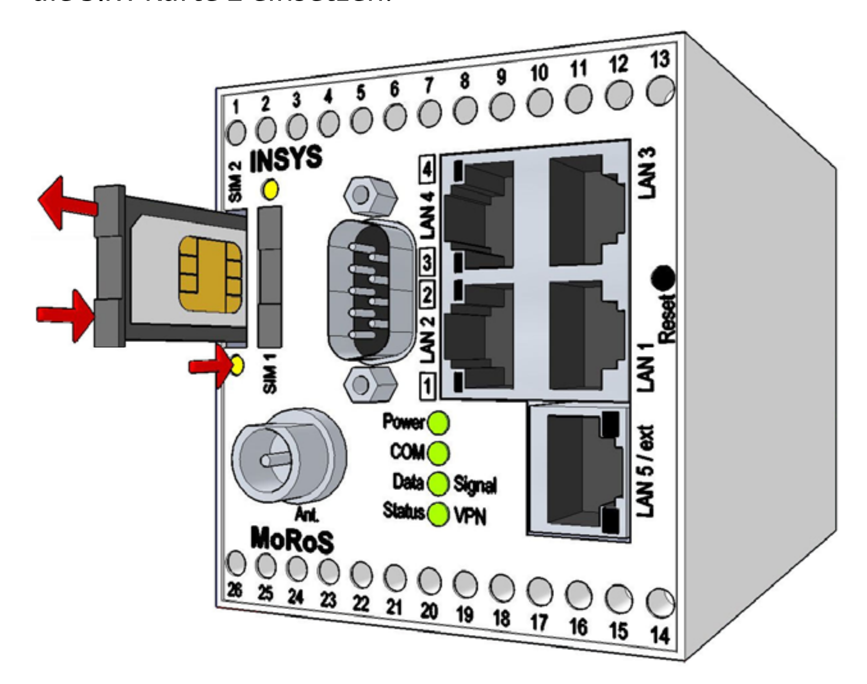
ⓘ Folgende Abbildung zeigt, wie Sie die SIM-Karte in den SIM-Kartenhalter für die SIM-Karte 1 einsetzen:



6. Schalten Sie die Stromversorgung des MoRoS UMTS PRO 2.0 wieder ein.

➢ *Alternativ können Sie eine zweite SIM-Karte im MoRoS UMTS PRO 2.0 verwenden. Der MoRoS UMTS PRO 2.0 verfügt dafür über einen zweiten SIM-Kartenhalter für die SIM-Karte 2.*

ⓘ Folgende Abbildung zeigt, wie Sie die SIM-Karte in den SIM-Kartenhalter für die SIM-Karte 2 einsetzen:



Den MoRoS UMTS PRO 2.0 an eine GSM-Antenne und einen PC anschließen

So verbinden Sie den MoRoS UMTS PRO 2.0 mit einer GSM-Antenne und über ein Netzwerkkabel mit einem PC.

⇢ Die Stromversorgung des MoRoS UMTS PRO 2.0 ist abgestellt.

⇢ Sie benötigen Cat. 5 . Netzwerk-Patchkabel.

⇢ Sie benötigen eine Netzwerkkarte am PC.

⇢ Sie benötigen eine passende GSM-Antenne (bei INSYS MICROLECTRONICS erhältlich.)

ⓘ Für die USA gilt die Vorschrift der Federal Communications Commission (FCC), nach der die Antenne in mindestens 20 cm Abstand zu Personen, nicht am gleichen Ort mit anderen Antennen oder Sendern installiert und betrieben werden sowie einen Antennengewinn von nicht mehr als 8,4 dBi (GSM 1900) beziehungsweise 2,9.dBi (GSM 850) aufweisen soll.

1. Suchen Sie die RJ-45-Buchse der Netzwerkkarte am PC.

2. Stellen Sie sicher, das die vermeintliche Buchse keine ISDN-Buchse ist, sondern die Buchse der Netzwerkkarte, dies Sie zur Konfiguration des MoRoS UMTS PRO 2.0 verwenden wollen.

3. Stecken Sie das einen Ende des Netzwerkkabels in die RJ-45-Buchse der PC-Netzwerkkarte und das andere Ende in eine Netzwerkbuchse am Switch des MoRoS UMTS PRO 2.0.

4. Schließen Sie die GSM-Antenne an die Antennenbuchse des MoRoS UMTS PRO 2.0 an.

Den MoRoS UMTS PRO 2.0 konfigurieren

⇢ Der MoRoS UMTS PRO 2.0 ist an den PC angeschlossen.

⇢ Die Spannungsversorgung des MoRoS UMTS PRO 2.0 ist eingeschaltet.

⇢ Sie haben die nötigen Zugriffsrechte, die IP-Adresse der Netzwerkkarte zu verändern, an die der MoRoS UMTS PRO 2.0 angeschlossen ist.

1. Ändern Sie die IP-Adresse der Netzwerkkarte, an die der MoRoS UMTS PRO 2.0 angeschlossen ist, auf eine Adresse die mit 192.168.1. beginnt.

➢ *Alternativ können Sie Ihre Netzwerkkarte auf „automatische Adresszuweisung“ konfigurieren. Der integrierte DHCP Server des MoRoS UMTS PRO 2.0 weist Ihrer Netzwerkkarte dann beim Anstecken eine Adresse aus dem passenden Adressbereich zu.*

ⓘ Verwenden Sie nicht die Adresse 192.168.1.1. Das ist die ab Werk eingestellte IP-Adresse des MoRoS UMTS PRO 2.0. Verwenden Sie z.B. 192.168.1.2. als IP-Adresse für die Netzwerkkarte in Ihrem PC.

2. Öffnen Sie einen Webbrowser, und richten Sie ihn auf die URL „http://192.168.1.1“

✓ Der Webbrowser lädt die Startseite des MoRoS UMTS PRO 2.0.

➢ *Falls Sie im Browserfenster die Meldung sehen, dass die Seite mit der Adresse nicht gefunden werden kann: Prüfen Sie, ob Ihr MoRoS UMTS PRO 2.0 mit Spannung versorgt ist. Falls ja, ist vermutlich die falsche IP-Adresse im MoRoS UMTS PRO 2.0 eingestellt. Drücken Sie dafür dreimal innerhalb von 2 Sekunden auf den Reset-Taster am MoRoS UMTS PRO 2.0 und wiederholen Sie diese Anleitung ab Schritt 2.*

✓ Sie werden durch einen Dialog zur Authentifizierung mit Benutzernamen und Passwort aufgefordert.

3. Geben Sie das als Benutzernamen „insys“ und als Passwort „moros“ ein.

ⓘ Benutzername und Passwort sind als Werkeinstellung gesetzt. Funktioniert die Anmeldung am Webinterface mit diesen Daten nicht, setzen Sie Ihren MoRoS UMTS PRO 2.0 einfach auf die Werkseinstellungen zurück.
Drücken Sie dafür dreimal innerhalb von 2 Sekunden auf den Reset-Taster am MoRoS UMTS PRO 2.0 und wiederholen Sie diese Anleitung ab Schritt 2.

✓ Sie sehen die Startseite des Webinterface.

✓ Der MoRoS UMTS PRO 2.0 ist erfolgreich installiert und bereit zur Konfiguration.

11 Bedienprinzip

Dieses Kapitel erklärt Ihnen, wie Sie bei Bedienung und Konfiguration eines MoRoS UMTS PRO 2.0 vorgehen.

Der MoRoS UMTS PRO 2.0 wird mit Hilfe einer webbasierten Oberfläche konfiguriert und bedient. Die Oberfläche selbst wird mit Hilfe eines Webbrowser wie Mozilla Firefox oder dem Microsoft Internet Explorer angezeigt und bedient.

11.1 Bedienung mit Weboberfläche

Die Weboberfläche ermöglicht eine komfortable Konfiguration des MoRoS UMTS PRO 2.0 mit Hilfe eines Webbrowsers. Über die Oberfläche ist es möglich, alle Funktionen des MoRoS UMTS PRO 2.0 zu konfigurieren. Die Bedienung ist weitgehend selbsterklärend. Die Oberfläche bietet zusätzlich eine Online-Hilfe, in der die Bedeutung möglicher Einstellungen des MoRoS UMTS PRO 2.0 erklärt ist. Aktivieren Sie die Online-Hilfe indem Sie in der Titelleiste unter der Sprachauswahl die Option „Hilfetexte anzeigen“ auswählen.

ⓘ Wir empfehlen bei den ersten Konfigurationsvorgängen unbedingt, die Online-Hilfe zu aktivieren, um eine schnelle und fehlerfreie Konfiguration zu ermöglichen.

Konfigurieren und Einstellen des MoRoS UMTS PRO 2.0 mit Weboberfläche

Hier erfahren Sie, wie Sie prinzipiell vorgehen, wenn Sie MoRoS UMTS PRO 2.0 mit der Weboberfläche konfigurieren.

- Der MoRoS UMTS PRO 2.0 ist an ein Netzwerk angeschlossen und eingeschaltet.
- Ein PC, der physikalisch mit demselben Netzwerk verbunden ist, mit dem auch der MoRoS UMTS PRO 2.0 verbunden ist.
- Der PC ist so konfiguriert, dass er sich auch logisch mit dem MoRoS UMTS PRO 2.0 im selben Netz befindet. Dafür müssen die ersten drei Stellen der IP-Adresse des PC und MoRoS UMTS PRO 2.0 gleich sein. Beispielsweise hat MoRoS UMTS PRO 2.0 die IP-Adresse 192.168.1.1. und der PC die IP-Adresse 192.168.1.2
- Ein Webbrowser neuerer Generation, wie z.B. Mozilla Firefox oder Microsoft Internet Explorer, ist auf dem PC installiert.

1. ***Starten Sie den Webbrowser.***
2. ***Geben Sie die IP-Adresse des MoRoS UMTS PRO 2.0 in die Adresszeile ein.***

ⓘ Die ab Werk voreingestellte IP-Adresse des MoRoS UMTS PRO 2.0 ist **192.168.1.1**.

✓ Ein Dialog zur Authentifizierung erscheint und fordert Sie auf, Benutzernamen und Passwort einzugeben.

3. ***Geben Sie den Benutzernamen und Passwort ein und klicken Sie danach auf OK.***

ⓘ Die Werkseinstellung der Weboberfläche für den
Benutzernamen ist **„insys“**, das
Passwort „moros“.

✓ Die Startseite der Weboberfläche wird angezeigt.

4. ***Wählen Sie über das Menü links den Menüpunkt aus, in dem Sie Einstellungen vornehmen möchten.***

5. ***Nehmen Sie die gewünschten Einstellungen vor.***

6. ***Klicken Sie abschließend auf die Schaltfläche OK auf der jeweiligen Konfigurationsseite, um die Einstellungen zu speichern.***

ⓘ Bitte klicken Sie nach einer Änderung der Konfiguration stets die auf die Schaltfläche OK, da ansonsten bei einem Wechsel der Seite oder beim Schließen des Browsers die Einstellungen verloren gehen.

11.2 Zugang über das HTTPS-Protokoll

Die Weboberfläche ermöglicht auch eine sichere Konfiguration des MoRoS UMTS PRO 2.0 unter Verwendung des HTTPS-Protokolls. Das HTTPS-Protokoll ermöglicht eine Authentifizierung des Servers (d.h. des MoRoS UMTS PRO 2.0) sowie eine Verschlüsselung der Datenübertragung.

Bei einem ersten Zugriff auf den MoRoS UMTS PRO 2.0 über das HTTPS-Protokoll zeigt der Browser an, dass der MoRoS UMTS PRO 2.0 ein ungültiges Sicherheitszertifikat verwendet. Dem Zertifikat wird nicht vertraut, weil das Aussteller-Zertifikat (CA-Zertifikat) unbekannt ist.

Sie können diese Warnmeldung ignorieren und (je nach Browser und Betriebssystem) eine Ausnahme für diesen Server hinzufügen oder die sichere Verbindung zu diesem Server trotzdem aufbauen.

Wir empfehlen, das CA-Zertifikat CA_MoRoS.crt von der Zertifikats-Seite (http://www.insys-tec.de/zertifikat/) herunterzuladen und in Ihren Browser zu importieren, um INSYS MICROELECTRONICS als Zertifizierungsstelle anzuerkennen. Gehen Sie dazu vor, wie in der Dokumentation Ihres Browsers beschrieben.

Wenn INSYS MICROELECTRONICS als Zertifizierungsstelle in Ihrem Browser hinterlegt ist und sie erneut auf den MoRoS UMTS PRO 2.0 über das HTTPS-Protokoll zugreifen, zeigt der Browser erneut an, dass der MoRoS UMTS PRO 2.0 ein ungültiges Sicherheitszertifikat verwendet. Dem Zertifikat wird nicht vertraut, weil sich der Common Name des Zertifikates von Ihrer Eingabe in der Adressleiste des Browsers unterscheidet. Der Browser meldet, dass sich ein anderes Gerät unter dieser URL meldet. Der Common Name des Zertifikates besteht aus der MAC-Adresse des MoRoS UMTS PRO 2.0, wobei die Doppelpunkte durch Unterstriche ersetzt sind.

Sie können diese Warnmeldung ignorieren und (je nach Browser und Betriebssystem) eine Ausnahme für diesen Server hinzufügen oder die sichere Verbindung zu diesem Server trotzdem aufbauen.

Um auch diese Browser-Warnung zu vermeiden, müssen Sie den Common Name des zu erreichenden MoRoS UMTS PRO 2.0 in die Adressleiste Ihres Browsers eingeben. Damit die URL zum richtigen Gerät führt, muss der Common Name mit der IP-Adresse des MoRoS UMTS PRO 2.0 verknüpft werden. Den Allgemeinen Namen (Common Name) können Sie herausfinden, indem Sie das Zertifikat vom MoRoS UMTS PRO 2.0 herunterladen und dies ansehen. Die Vorgehensweise hierzu ist von Ihrem Browser abhängig. Die Vorgehensweise für das Einrichten der Verknüpfung ist abhängig von Ihrem Betriebssystem:

- Editieren von /etc/hosts (Linux/Unix)
- Editieren von C:\WINDOWS\system32\drivers\etc\hosts (Windows XP)
- Konfigurieren Ihres eigenen DNS-Servers

Sehen Sie für weitere Informationen dazu in der Dokumentation Ihres Betriebssystems nach.

12 Funktionen

12.1 Basic Settings

12.1.1 Webinterface (Benutzername, Kennwort, Fernkonfiguration)

Die Weboberfläche dient zur Konfiguration des MoRoS UMTS PRO 2.0. Sie wird durch eine Benutzername / Kennwortabfrage gegen unbefugte Zugriffe geschützt. Die Weboberfläche kann für eine Konfiguration von einem Rechner aus dem internen Netz oder für eine Fernkonfiguration konfiguriert werden. Dann erreichen Sie die Weboberfläche auch aus dem externen Netz. Eine Fernkonfiguration kann auch über das HTTPS-Protokoll erfolgen. Für eine bessere Unterscheidbarkeit kann ein Standort eingetragen werden. Sie können den Port festlegen, unter dem Sie die Oberfläche aus dem jeweiligen Netz des MoRoS UMTS PRO 2.0 erreichen.

Konfiguration mit Weboberfläche

Benutzernamen und Kennwort geben Sie im Menü „Basic Settings“ auf der Seite „Webinterface“ im Feld „Authentifizierung“ ein.

Die **zulässige Konfiguration** aktivieren Sie über die jeweilige Checkbox.

Eine **Bezeichnung des Routers oder Standorts** kann im Feld „Standort“ eingegeben werden. Diese Bezeichnung erscheint dann in der Titelzeile des Browserfensters sowie der Startseite der Weboberfläche und erleichtert eine Unterscheidung wenn mehrere Weboberflächen-Fenster geöffnet sind.

Den **Port der Weboberfläche** legen Sie im Eingabefeld „HTTP Port der Weboberfläche“ bzw. „HTTPS Port der Weboberfläche“ fest. Standardmäßig ist Port 80 (HTTP) bzw. Port 443 (HTTPS) für die Weboberfläche des MoRoS UMTS PRO 2.0 eingestellt.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.1.2 IP-Adressen einstellen oder per DHCP beziehen

Der MoRoS UMTS PRO 2.0 muss im LAN unter einer bestimmten IP-Adresse erreichbar sein. Dazu müssen Sie eine statische IP-Adresse eingeben.

Konfiguration mit Weboberfläche

Um eine **statische IP-Adresse** einzustellen, wechseln Sie im Menü „Basic Settings“ auf die Seite „IP-Adresse (LAN)“.

Geben Sie im Eingabefeld „IP-Adresse“ die **IP-Adresse** des MoRoS UMTS PRO 2.0 im LAN sowie im Feld „Netzmaske“ die **Netzmaske** ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Die **MAC-Adresse des MoRoS UMTS PRO 2.0** finden Sie unter den Eingabefeldern für die IP-Adresse und Netzmaske unter „MAC-Adresse“ auf dieser Seite.

ⓘ Der Link „DHCP-Server Einstellungen anpassen“ am Ende der Seite erinnert daran, auch diese Einstellungen anzupassen, wenn die IP-Adresse geändert wird.

12.1.3 Statische Routen eintragen

Sie können im MoRoS UMTS PRO 2.0 statische Routen für die Weiterleitung von Datenpaketen definieren, die beim Systemstart geladen werden.

Konfiguration mit Weboberfläche

Um eine **statische Route** einzutragen, wechseln Sie im Menü „Basic Settings“ auf die Seite „Routing“.

Geben Sie im Abschnitt „Neue Route hinzufügen“ die **Netzwerkadresse**, die **Netzmaske** sowie das **Gateway** in die jeweiligen Felder ein.

Um eine **bestehende Route zu löschen**, aktivieren Sie unter „Bestehende Routen“ die Checkbox der Route(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

ⓘ Hier kann weder ein Default-Gateway eingetragen werden, noch kann NAT ein- oder ausgeschaltet werden. Dies wird bei der jeweiligen Schnittstelle in den Menüs „Dial-In“, „Dial-Out“ bzw. „Lan (ext)“ auf der dortigen Seite „Routing“ konfiguriert.

12.2 UMTS

12.2.1 PIN der SIM-Karte eingeben

Das MoRoS UMTS PRO 2.0 ermöglicht die Verwendung von zwei SIM-Karten. Beim Betrieb mit nur einer einzigen SIM-Karte muss diese in den Kartenhalter für die SIM-Karte 1eingelegt sein. Zusätzlich kann noch eine zweite SIM-Karte in den Kartenhalter für die SIM-Karte 2 eingesetzt werden. Ein Betrieb mit einer SIM-Karte in SIM 2 ohne einer SIM-Karte in SIM 1 ist nicht vorgesehen.

Damit MoRoS UMTS PRO 2.0 sich ins Mobilfunknetz einbuchen und CSD- bzw. IP-Verbindungen aufbauen kann, benötigt er (sofern die SIM-Karte mit einer PIN geschützt ist) die PIN der eingesetzten SIM-Karte.

Hinweis!



Mögliche Sperrung der SIM-Karte!

Durch Eingeben einer falschen PIN kann die SIM-Karte gesperrt werden und damit MoRoS UMTS PRO 2.0 sich nicht mehr ins Mobilfunknetz einbuchen.

Achten Sie beim Eingeben oder Ändern der PIN darauf, die richtige PIN für die SIM-Karte einzugeben. Die SIM-Karte kann mit der zugehörigen PUK wieder entsperrt werden. Zum Entsperren mit der PUK benötigen Sie ein Mobiltelefon, in das Sie die gesperrte SIM-Karte einsetzen und die PUK eingeben können. Alternativ können Sie die SIM-Karte mit dem Befehl **`AT+CPIN=PUK,NEW_PIN`** im Terminal entsperren.

Konfiguration mit Weboberfläche

Geben Sie die **PIN der eingesetzten SIM-Karte** im Menü „UMTS“ in das Eingabefeld „PIN“ für die jeweilige SIM-Karte (1 oder 2) ein. Geben Sie zur Bestätigung der korrekten Eingabe die PIN noch einmal in das Feld „PIN-Wiederholung“ ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

ⓘ Die Eingabe einer PIN wird auch dann gespeichert, wenn die Freischaltung der SIM-Karte nicht erfolgreich war. Das ist erlaubt, um eine Konfiguration auch ohne eingelegte SIM-Karte zu ermöglichen. Aus diesem Grund wird auch eine falsche PIN gespeichert!

12.2.2 Netzwahl einstellen

Sie können bestimmen, in welches Mobilfunknetz sich der MoRoS UMTS PRO 2.0 einbucht. Dazu muss Ihre SIM-Karte Roaming unterstützen. Der MoRoS UMTS PRO 2.0 kann sich dann mit dem am Standort am stärksten empfangbaren Netz, mit einem bestimmten bevorzugten Netz (das nicht unbedingt das am besten empfangene Netz sein muss) oder ausschließlich mit dem Netz eines bestimmten Providers verbinden. Bestimmen Sie einen „bevorzugte Provider“, wird der MoRoS UMTS PRO 2.0 versuchen, sich immer mit dem Netz dieses Providers zu verbinden. Schlägt der Verbindungsversuch zum Netz des bevorzugten Providers fehl, bucht sich der MoRoS UMTS PRO 2.0 in das am besten empfangbare Netz irgendeines Providers ein. Diese Einstellungen erfolgen für jede SIM-Karte getrennt.

Konfiguration mit Weboberfläche

Um die **Art der Netzwahl auszuwählen**, wählen Sie im Menü „UMTS“ über Radiobuttons, ob sich die jeweilige SIM-Karte (1 oder 2) des MoRoS UMTS PRO 2.0 ins stärkste Netz, bei einem bevorzugten Provider und dessen Netz oder ausschließlich im Netz eines von Ihnen bestimmten Providers einbuchen soll.

Damit sich der **MoRoS UMTS PRO 2.0 bevorzugt beim Netz eines bestimmten Providers einbucht**, wählen Sie im Menü „UMTS“ den Radiobutton für die Option „Bevorzugt bei diesem Provider einbuchen“. Geben Sie die Nummer des Providers im Eingabefeld dahinter an. Die Nummer des Providers können Sie über den Link unter dem Fragezeichen neben „Providerliste aus dem Modem auslesen…“ herausfinden (das Fragezeichen erscheint nur, wenn eine SIM-Karte eingelegt und mit der richtigen PIN entsperrt wurde). Um die Daten auslesen zu können, muss eine SIM Karte eingelegt sein und der MoRoS UMTS PRO 2.0 muss in ein GSM/UMTS-Netz eingebucht sein.

Damit sich der **MoRoS UMTS PRO 2.0 ausschließlich beim Netz eines bestimmten Providers einbucht**, wählen Sie im Menü „UMTS“ den Radiobutton für die Option „Ausschließlich bei diesem Provider einbuchen“. Geben Sie die Nummer des Providers im Eingabefeld dahinter an. Die Nummer des Providers können Sie über den Link unter dem Fragezeichen neben „Providerliste aus dem Modem auslesen…“ herausfinden (das Fragezeichen erscheint nur, wenn eine SIM-Karte eingelegt und mit der richtigen PIN entsperrt wurde).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.2.3 Tägliches Aus- und Einbuchen einstellen

Der MoRoS UMTS PRO 2.0 kann sich innerhalb von 24 Stunden zu bestimmten Uhrzeiten in das Mobilfunknetz aus- und auch zeitgesteuert wieder einbuchen. So können Sie die Verbindung auf bestimmte Zeiten begrenzen. Durch das periodische Aus- und Einbuchen erhöhen Sie die Verfügbarkeit des MoRoS UMTS PRO 2.0, die sonst durch verschiedene Umstände, bei denen ein Neueinbuchen ins Netz erforderlich wäre, beinträchtig sein könnte, z.B. Wartungsarbeiten in den Mobilfunknetzen, die ein erneutes Einbuchen erforderlich machen. Wir empfehlen Ihnen die Verwendung dieser Funktion.

ⓘ Es wird unbedingt empfohlen, den MoRoS UMTS PRO 2.0 täglich in das Mobilfunknetz neu einzubuchen, um eine hohe Verfügbarkeit zu erreichen.

Konfiguration mit Weboberfläche

Geben Sie die **gewünschte Uhrzeit für das tägliche Ausbuchen** im Menü „UMTS“ in die Eingabefelder „Tägliches Ausbuchen um“ im Format „hh:mm“ ein.

Geben Sie die **gewünschte Uhrzeit für das tägliche Einbuchen** im Menü „UMTS“ in die Eingabefelder „Tägliches Einbuchen um“ im Format „hh:mm“ ein.

Schalten Sie die Funktion ein durch Aktivieren der Checkbox „Tägliches Aus- und Einbuchen aktivieren“.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.2.4 Terminal

Diese Funktion ermöglicht die direkte Übermittlung von AT-Befehlen an das Kommunikationsgerät des MoRoS UMTS PRO 2.0. Die Anzeige der Antwort erfolgt direkt unterhalb des Eingabefelds.

Konfiguration mit Weboberfläche

Geben Sie den **gewünschten AT-Befehl** im Menü „UMTS“ im Abschnitt „Terminal“ in das Eingabefeld „AT-Kommando“ ein.

Übermitteln Sie den Befehl, indem Sie auf „OK“ klicken.

12.3 Dial-In

12.3.1 Dial-In-Server einrichten

Sie können den MoRoS UMTS PRO 2.0 als Einwahl-Server bzw. eingehenden PPP-Server verwenden. Die Dial-In-Funktion ermöglicht, dass sich Benutzer aus der Ferne per Modem über den MoRoS UMTS PRO 2.0 mit dem Netzwerk hinter dem MoRoS UMTS PRO 2.0 verbinden. Ähnlich der Einwahl bei einem Internetprovider authentifizieren sich die Benutzer per Benutzernamen und Kennwort beim MoRoS UMTS PRO 2.0. Zur Authentifizierung der PPP-Nutzer stehen die Methoden PAP oder CHAP zur Verfügung. Erfolgreich authentifizierte Nutzer können eine PPP-Verbindung aufbauen, um auf das Netzwerk des MoRoS UMTS PRO 2.0 zuzugreifen.

Konfiguration mit Weboberfläche

Um den **Dial-In**-Server zu **aktivieren**, wählen Sie im Menü „Dial-In" auf der Seite „Dial-In" den Radiobutton „Ja" für „Dial-In aktivieren".

Sie können eine **Leerlaufzeit** bestimmen, nach der Einwahlverbindungen geschlossen werden, sobald kein Datentransfer mehr stattfindet. Geben Sie die Zeit in Sekunden in das Eingabefeld „Idle Time" ein. Wenn die Verbindung trotz Leerlauf aufrecht erhalten werden soll, geben Sie den Wert „0" ein.

Legen Sie die **Zahl der Klingelzeichen** fest, nach den der MoRoS UMTS PRO 2.0 einen Anruf entgegennimmt. Geben Sie die Anzahl der Klingelzeichen bis zum Abheben in das Eingabefeld „Klingelzeichen bis zur Anrufannahme" ein.

Um eine **Benutzernamen- und Passwort-basierte PPP-Authentifizierung** zu verwenden, aktivieren Sie die Checkbox „Authentifizierung für Dial-In". Wenn Sie diese Checkbox deaktiveren, kann jeder Anrufer eine PPP Verbindung aufbauen. Geben Sie bis zu 10 verschiedene **Kombinationen aus Benutzername und Passwort** in die Felder „Benutzername" und Passwort" ein und legen Sie über den jeweiligen Radiobutton fest, ob für diesen Benutzer eine **Authentifizierung per „PAP" oder „CHAP"** erfolgen soll.

Wenn für den jeweiligen Benutzer ein **Callback nach erfolgreicher Authentifizierung** möglich sein soll, aktivieren Sie die Checkbox „Rückruf aktiv". Wenn bei einem Callback die Authentifizierung notwendig ist, aber hier kein Häkchen gesetzt ist, dann erfolgt auch kein Callback. In dem Fall wird dem Anrufer ein gewöhnlicher Dial-In ermöglicht.

Optional können Sie die **IP-Adressen der Endpunkte der PPP-Verbindung** festlegen, falls diese Adressen in einem der Netzwerke am MoRoS UMTS PRO 2.0 oder an der Gegenstelle schon vergeben sind. Standardmäßig ist die IP-Adresse des MoRoS UMTS PRO 2.0 die 192.168.254.1. Die Standard-Adresse der Gegenstelle ist 192.168.254.2.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK" klicken.

12.3.2 Automatischer Rückruf (Callback)

Sie können einen automatischen Rückruf zu einer vordefinierten Zielrufnummer des MoRoS UMTS PRO 2.0 mit einem Datenanruf oder Telefonanruf auslösen. Die Anrufer können sich über die PPP-Authentifizierungsmethoden PAP oder CHAP identifizieren. Die Verbindung, die dann vom MoRoS UMTS PRO 2.0 aufgebaut wird, müssen Sie zuvor im Menü „Dial-Out" konfigurieren. Es sind ausschließlich Verbindungen zum vorkonfigurierten Dial-Out Ziel möglich.

Konfiguration mit Weboberfläche

Um eine **Dial-Out Verbindung durch einen Anrufer auszulösen**, aktivieren Sie im Menü „Dial-In" auf der Seite „Dial-In" die Checkbox „Automatischen Rückruf nach erfolgreicher PPP-Authentifikation aktiveren". Die Dial-Out-Verbindung, die durch einen Anrufer ausgelöst wird, muss dafür zuvor im Menü „Dial-Out" konfiguriert sein.
Speichern Sie Ihre Einstellungen, indem Sie auf „OK" klicken.

12.3.3 Routing

Sie können im MoRoS UMTS PRO 2.0 Routen für die Weiterleitung von Datenpaketen definieren. Weiterhin können Sie NAT getrennt für eingehende und ausgehende Pakete aktivieren.

Konfiguration mit Weboberfläche

Um eine **Default-Route zu setzen**, aktivieren Sie im Menü „Dial-In" auf der Seite „Routing" die Checkbox „Default Route setzen".

Um **NAT für eingehende Pakete zu aktivieren**, aktivieren Sie im Menü „Dial-In" auf der Seite „Routing" die Checkbox „NAT für eingehende Pakete aktivieren".

Um **NAT für ausgehende Pakete zu aktivieren**, aktivieren Sie im Menü „Dial-In" auf der Seite „Routing" die Checkbox „NAT für ausgehende Pakete aktivieren".

Um eine **neue Route hinzuzufügen**, geben Sie im Menü „Dial-In" auf der Seite „Routing" die „Netzwerkadresse" und die „Netzwerkmaske" in die jeweiligen Felder ein.

Um eine **bestehende Route zu löschen**, aktivieren Sie im Menü „Dial-In" auf der Seite „Routing" unter „Bestehende Routen" die Checkbox der Route(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK" klicken.

12.3.4 Firewall-Regel erstellen oder löschen

Der MoRoS UMTS PRO 2.0 bietet eine Firewall für Dial-In-Verbindungen. Eine Firewall dient dazu, unerwünschten Datenverkehr zu verhindern. Die Logik der Firewall ist, dass jeglicher Datenverkehr verboten ist, der nicht explizit durch eine Regel erlaubt wurde.

Hier definieren Sie, welche Verbindungen über den MoRoS UMTS PRO 2.0 zugelassen sind. Wenn Sie die Firewall für die Verbindungsart „Dial-In“ einschalten, sind nur noch Verbindungen möglich, die durch Firewallregeln erlaubt werden. Alle anderen Verbindungen werden blockiert.

Konfiguration mit Weboberfläche

Um die **Firewall für Dial-In-Verbindungen zu aktivieren**, aktivieren Sie im Menü „Dial-In“ auf der Seite „Firewall“ die Checkbox „Firewall für Dial-In-Verbindungen aktivieren“.

Um eine **Regel für eine zugelassene IP-Verbindung zu erstellen**, gehen Sie wie folgt vor.

Wählen Sie im Menü „Dial-In“ auf der Seite „Firewall“ im Dropdown-Menü „Datenrichtung“ für die Regel eine **Datenrichtung** aus.

Bestimmen Sie das **Protokoll der zugelassenen Verbindung** im Dropdownmenü „Protokoll“.

Sie können zusätzlich dafür sorgen, dass die Regel **ausschließlich für einen bestimmten Dial-In-Benutzer angewandt wird**; wählen Sie hierzu im Drowdownmenü „Dial-In Benutzername“ den entsprechenden Dial-In-Benutzernamen aus.

Geben Sie in den Eingabefeldern „**Absender-IP-Adresse**“, „**Ziel-IP-Adresse**“ und **Ziel-Port** die weiteren Spezifikationen für die zugelassen Verbindungen durch den MoRoS UMTS PRO 2.0 an. Es können Regeln erstellt werden, die nicht nur für einzelne Maschinen (Hosts) gelten, sondern für ganze Netze. In dem Fall muss die Netzwerkmaske nach dem „/“ eingegeben werden.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **Firewall-Regeln temporär auszuschalten**, deaktivieren Sie im Menü „Dial-In“ auf der Seite „Firewall“ die Checkbox in der Spalte „aktiv“ in der Übersicht der Firewallregeln. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **eine oder mehrere Regeln** zu **löschen**, aktivieren Sie die Checkbox in der Spalte „löschen“ in der Übersicht der Firewallregeln. Klicken Sie auf „OK“, um die Einstellung zu übernehmen.

12.4 Dial-Out

12.4.1 Dial-Out einrichten

Sie können den MoRoS UMTS PRO 2.0 für den Dial-Out einsetzen. Der MoRoS UMTS PRO 2.0 stellt automatisch eine PPP-Verbindung zu einer Gegenstelle her, wenn Netzwerkverkehr in Richtung des Netzes der Gegenstelle auftritt. Der Netzwerkverkehr, der einen Verbindungsaufbau auslösen darf, kann über Regeln beschränkt werden. Dieser optionale „Wählfilter“ sorgt dafür, dass nur Pakete von bzw. zu bestimmten IP-Adressen oder von bzw. zu bestimmten Ports die Dial-Out-Verbindung auslösen. Diese Dial-Out Verbindung ist vergleichbar mit der Einwahl eines PC ins Internet. Erst nach dieser Einwahl ist es möglich, IP-Daten (z.B. Webinhalte) zu übertragen oder z.B. aus der Ferne auf Geräte im lokalen Netz des MoRoS UMTS PRO 2.0 zuzugreifen.

Konfiguration mit Weboberfläche

Um den **Dial-Out einzuschalten**, wählen Sie in Menü „Dial-Out“ auf der Seite „Dial-Out“ in der Auswahl „Dial-Out aktivieren“ die Option „Ja“.

Geben Sie für eine **GSM-CSD-Verbindung die Rufnummer der PPP-Gegenstelle** (z.B. den Internetprovider) in das Eingabefeld „Rufnummer“ für Ziel A ein. Sie können eine weitere Rufnummer (oder „*99***1#“ für eine paketbasierte Verbindung, siehe unten) bei Ziel B eingeben.

Geben Sie für eine **paketbasierte Verbindung (GPRS/EDGE/UMTS/HSDPA)** in das Eingabefeld bei „Rufnummer“ für Ziel A „*99***1#“ ein. Geben Sie für Ziel A den APN Ihres Mobilfunkproviders in das Feld „Access Point Name“ ein, über den die paketbasierte Verbindung aufgebaut werden soll. Sie können einen weiteren APN bei Ziel B eingeben. Alternativ können Sie für Ziel B auch eine GSM-CSD-Verbindung mit einer gewöhnlichen Rufnummer definieren.

Geben Sie **Benutzername und Passwort** für die PPP-Einwahl-Ziele A und B an. Die Angabe des Ziels B ist optional.

Wählen Sie für Ziel A und B die jeweils zu verwendende **PPP-Authentifizierungsmethode (PAP; CHAP, und PAP oder CHAP)** in der Auswahl „Authentifizierung“ aus.

Falls Sie eine zweite SIM-Karte verwenden, können Sie unter „Sim-Karte für Ziel B“ die **für Ziel B zu verwendende SIM-Karte auswählen**. Für Ziel A wird immer die SIM-Karte 1 verwendet.

Über die „**Idle Time**“ können Sie bestimmen, wie lange die Verbindung aufrecht erhalten wird, wenn kein Datentransfer mehr stattfindet. Geben Sie die gewünschte Leerlaufzeit in das Eingabefeld „Idle Time“ in Sekunden ein.
Um die Verbindung unbegrenzt lange zu halten geben Sie als Zeit den Wert „0“ ein.

Über die **maximale Verbindungszeit** können Sie die Dauer einer Verbindung beschränken. Geben Sie eine maximale Verbindungszeit an, wird die Verbindung nach Ablauf dieser Zeit geschlossen. Um die Verbindung zeitlich unbegrenzt (bis zum Verbindungsabbau aus anderen Gründen) geöffnet zu lassen, geben Sie als Zeit den Wert „0“ in das Eingabefeld „maximale Verbindungszeit“ ein.

Die **Priorität der Ziele** konfigurieren Sie unter „Priorität“. Dazu stehen Ihnen die Optionen „Zuletzt erfolgreiches Ziel zuerst versuchen“ oder „Immer Ziel A zuerst versuchen“ zur Verfügung. Der MoRoS UMTS PRO 2.0 wird das jeweilige Ziel zuerst verwenden. Funktioniert der Verbindungsaufbau zu diesem Ziel nicht, so versucht der MoRoS UMTS PRO 2.0 das andere Ziel zu erreichen.

Falls dem Router bei einem Dial-Out keine IP-Adresse für einen zu benutzenden DNS-Server mitgeteilt wird, muss die Checkbox "DNS-Server-Adresse anfordern" deaktiviert werden. Ansonsten kann eventuell keine Verbindung zustande kommen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.4.2 Standleitungsbetrieb einrichten

Sie können den MoRoS UMTS PRO 2.0 so einstellen, dass eine PPP-Verbindung dauerhaft aufrecht erhalten bleibt. Diese Betriebsart ist interessant für private Netze, bei denen keine Minutengebühren anfallen, oder für Abrechnungsmodelle, in denen nur die übertragenen Datenvolumen bezahlt werden (z.B. paketbasierte Netze). Der MoRoS UMTS PRO 2.0 baut in diesem Betriebsmodus die Verbindung sofort nach dem Einschalten auf. Der MoRoS UMTS PRO 2.0 prüft die Verbindung periodisch auf ihre Funktion. Die Verbindungsprüfung kann entweder über eine DNS-Abfrage eines Hostnamens oder über Ping an einen Host durchgeführt werden.

Konfiguration mit Weboberfläche

Um die **Standleitung einzurichten**, aktivieren Sie im Menü „Dial-Out“ auf der Seite „Dial-Out“ die Checkbox „Verbindung sofort aufbauen und dauerhaft halten“.

Geben Sie, falls notwendig, eine andere Zeit in Minuten zur **Verbindungsprüfung** in das Eingabefeld „Zeitintervall der Verbindungsprüfung“ ein. Die Werkseinstellung ist 60 Minuten. Wird nach dieser Zeit eine geschlossene Verbindung festgestellt, versucht der MoRoS UMTS PRO 2.0 nach einer Minute die Verbindung neu aufzubauen. Schlägt der Versuch fehl, wird nach 5 Minuten erneut versucht, die Verbindung neu aufzubauen. Der nächste Versuch findet nach 30 Minuten statt, schlägt auch dieser Versuch fehl, versucht der MoRoS UMTS PRO 2.0 alle 60 Minuten die Verbindung neu aufzubauen.

Wählen Sie die **Methode zur Verbindungsprüfung** in der Auswahl „Art der Verbindungsprüfung“ aus und geben Sie einen Hostnamen oder eine „IP-Adresse“ an. Die beiden Methoden unterscheiden sich in Ihrer Wirkung. Ein fehlgeschlagener DNS-Request beendet eine evtl. bestehende Verbindung und baut diese neu auf. Ein fehlgeschlagener Ping sorgt dafür, dass die Verbindung neu initiiert wird, falls sie seit dem letzten Datenpaket oder Ping geschlossen wurde. Ein Abbau einer existierenden Verbindung findet nicht statt, falls der Ping nicht beantwortet wird.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.4.3 Periodischen Dial-Out-Verbindungsaufbau einrichten

Der MoRoS UMTS PRO 2.0 kann die zuvor konfigurierte Dial-Out-Verbindung zeitgesteuert auf und abbauen. Die Dial-Out-Verbindung wird täglich zu einer bestimmten Uhrzeit aufgebaut und zu einer anderen Uhrzeit wieder abgebaut.

Mit dieser Funktion werden jeweils einzelne Ereignisse ausgelöst, es wird keine Sperrzeit o.ä. definiert. Beispiel: Wenn ein Ausbuchen um 14:00 Uhr und ein automatisches Einbuchen um 16:00 Uhr definiert wird, so können andere Ereignisse auch innerhalb dieses Zeitraums einen Verbindungsaufbau (Dial-Out) auslösen, z.B. ein einfaches Paket, dass dem Wählfilter entspricht. Ebenso wird nach einem automatischen Einbuchen die Verbindung automatisch abgebaut, falls z.B. die konfigurierte „Idle Time“ abgelaufen ist.

Konfiguration mit Weboberfläche

Um eine **Verbindung zu einer bestimmten Uhrzeit täglich aufzubauen**, aktivieren Sie im Menü „Dial-Out“ auf der Seite „Dial-Out“ die Checkbox „Verbindung täglich automatisch aufbauen um“ und geben Sie eine Uhrzeit für den Verbindungsaufbau in die Eingabefelder für Stunden und Minuten ein.

Um eine **Verbindung zu einer bestimmten Uhrzeit täglich abzubauen**, aktivieren Sie im Menü „Dial-Out“ auf der Seite „Dial-Out“ die Checkbox „Verbindung täglich automatisch abbauen um“ und geben Sie eine Uhrzeit für den Verbindungsabbau in die Eingabefelder für Stunden und Minuten ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.4.4 Routing

Sie können im MoRoS UMTS PRO 2.0 Routen für die Weiterleitung von Datenpaketen definieren. Weiterhin können Sie NAT getrennt für eingehende und ausgehende Pakete aktivieren.

Konfiguration mit Weboberfläche

Um eine **Default-Route zu setzen**, aktivieren Sie im Menü „Dial-Out“ auf der Seite „Routing“ die Checkbox „Default Route setzen“.

Um **NAT für eingehende Pakete zu aktivieren**, aktivieren Sie im Menü „Dial-Out“ auf der Seite „Routing“ die Checkbox „NAT für eingehende Pakete aktivieren“.

Um **NAT für ausgehende Pakete zu aktivieren**, aktivieren Sie im Menü „Dial-Out“ auf der Seite „Routing“ die Checkbox „NAT für ausgehende Pakete aktivieren“.

Um eine **neue Route hinzuzufügen**, geben Sie im Menü „Dial-Out“ auf der Seite „Routing“ die „Netzwerkadresse“ und die „Netzwerkmaske“ in die jeweiligen Felder ein.

Um eine **bestehende Route zu löschen**, aktivieren Sie im Menü „Dial-Out“ auf der Seite „Routing“ unter „Bestehende Routen“ die Checkbox der Route(n), die gelöscht werden soll(en).

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.4.5 Wählfilter einrichten

Um unnötige Kosten durch unerwünschte Dial-Out-Vorgänge zu verhindern kann optional ein Wählfilter aktiviert werden. Mit diesem Wählfilter kann der Netzwerkverkehr beschränkt werden, der einen Dial-Out Vorgang auslösen kann. Sobald eine Dial-Out Verbindung aufgebaut ist, können allerdings alle Teilnehmer im Netzwerk auf die Dial-Out Verbindung zugreifen und IP-Daten übertragen.

Hier definieren Sie, welche Pakete die Dial-Out Verbindung über den MoRoS UMTS PRO 2.0 initiieren dürfen. Wenn Sie den Wählfilter einschalten, sind nur noch Dial-Out Verbindungen möglich, die durch Wählfilterregeln erlaubt werden. Alle andern Verbindungen werden blockiert.

Konfiguration mit Weboberfläche

Um den **Wählfilter einzuschalten**, aktivieren Sie im Menü „Dial-Out“ auf der Seite „Wählfiler“ die Checkbox „Wählfilter für Dial-Out-Verbindungen aktivieren“.

Um eine **Regel für einen Wählfilter zu erstellen**, gehen Sie wie folgt vor.

Wählen Sie im Menü „Dial-In“ auf der Seite „Firewall“ das **Protokoll der zugelassenen Verbindung** im Dropdownmenü „Protokoll“.

Geben Sie in den Eingabefeldern „**Absender-IP-Adresse**“, „**Ziel-IP-Adresse**“ und „**Ziel-Port“** die weiteren Spezifikationen für die zugelassen Verbindungen durch den MoRoS UMTS PRO 2.0 an. Es können Regeln erstellt werden, die nicht nur für einzelne Maschinen (Hosts) gelten, sondern für ganze Netze. In dem Fall muss die Netzwerkmaske nach dem „/“ eingegeben werden.

Um DNS-Anfragen an den Router, die einen Verbindungsaufbau initiieren würden (DNS-Relay), explizit zu erlauben, aktivieren Sie die Checkbox „DNS-Anfragen der Absender-IP-Adresse dürfen eine Verbindung initiieren“.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um einzelne **Dial-Out-Regeln temporär auszuschalten**, deaktivieren Sie im Menü „Dial-Out“ auf der Seite „Wählfilter“ die Checkbox in der Spalte „aktiv“ im Abschnitt „Diese Datenpakete dürfen einen Dial-Out initiieren“. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

Um **eine oder mehrere Regeln** zu **löschen**, aktivieren Sie die Checkbox in der Spalte „löschen“ im Abschnitt „Diese Datenpakete dürfen einen Dial-Out initiieren“. Klicken Sie auf „OK“ um die Einstellung zu übernehmen.

12.4.6 Firewall-Regel erstellen oder löschen

Der MoRoS UMTS PRO 2.0 bietet eine Firewall für Dial-Out-Verbindungen. Eine Firewall dient dazu, unerwünschten Datenverkehr zu verhindern. Die Logik der Firewall ist, dass jeglicher Datenverkehr verboten ist, der nicht explizit durch eine Regel erlaubt wurde.

Hier definieren Sie, welche Verbindungen über den MoRoS UMTS PRO 2.0 zugelassen sind. Wenn Sie die Firewall für die Verbindungsart „Dial-Out" einschalten, sind nur noch Verbindungen möglich, die durch Firewallregeln erlaubt werden. Alle anderen Verbindungen werden blockiert.

Konfiguration mit Weboberfläche

Um die **Firewall für Dial-Out-Verbindungen zu aktivieren**, aktivieren Sie im Menü „Dial-Out" auf der Seite „Firewall" die Checkbox „Firewall für Dial-Out-Verbindungen aktivieren".

Um eine **Regel für eine zugelassene IP-Verbindung zu erstellen**, gehen Sie wie folgt vor.

Wählen Sie im Menü „Dial-Out" auf der Seite „Firewall" im Dropdown-Menü „Datenrichtung" für die Regel eine **Datenrichtung** aus.

Bestimmen Sie das **Protokoll der zugelassenen Verbindung** im Dropdownmenü „Protokoll".

Geben Sie in den Eingabefeldern „**Absender-IP-Adresse**", „**Ziel-IP-Adresse**" und „**Ziel-Port**" die weiteren Spezifikationen für die zugelassen Verbindungen durch den MoRoS UMTS PRO 2.0 an. Es können Regeln erstellt werden, die nicht nur für einzelne Maschinen (Hosts) gelten, sondern für ganze Netze. In dem Fall muss die Netzwerkmaske nach dem „/" eingegeben werden.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK" klicken.

Um einzelne **Firewall-Regeln temporär auszuschalten**, deaktivieren Sie im Menü „Dial-Out" auf der Seite „Firewall" die Checkbox in der Spalte „aktiv" in der Übersicht der Firewallregeln. Klicken Sie auf „OK" um die Einstellung zu übernehmen.

Um **eine oder mehrere Regeln** zu **löschen**, aktivieren Sie die Checkbox in der Spalte „löschen" in der Übersicht der Firewallregeln. Klicken Sie auf „OK", um die Einstellung zu übernehmen.

12.4.7 Portforwarding- Regel erstellen

Bei Einbeziehung des Internets als Kommunikationsnetzwerk werden private und öffentliche IP-Adressen unterschieden. Um auf die in lokalen Netzwerken meist verwendeten privaten IP-Adressen aus dem Internet zugreifen zu können werden die Techniken NAT und Portforwarding benutzt. Im Internet ist nur die öffentliche IP-Adresse des MoRoS UMTS PRO 2.0 erreichbar. Über diese IP-Adresse können die lokalen Endgeräte im Netz des MoRoS UMTS PRO 2.0 aber trotzdem aus dem Internet erreicht werden, wenn NAT und Portforwarding benutzt werden.

Der MoRoS UMTS PRO 2.0 ermöglicht Portforwarding. Der MoRoS UMTS PRO 2.0 leitet von außen eingehende Pakete an bestimmte Rechner im Netzwerk um. Abgehende Pakete dieser Verbindungen aus dem Netzwerk werden umgekehrt wieder zu ihren Zielen

außerhalb des Netzes zurückgeleitet. Der MoRoS UMTS PRO 2.0 leitet an bestimmten Ports eingehende Datenpakete an jeweils einen Port einer bestimmten Zieladresse weiter. Über Regeln können Sie definieren, welche Pakete von außen an welche Adressen und Ports im Netzwerk umgeleitet werden. So können Sie bestimmte Dienste an Rechner im Netzwerk über das Telefonnetz zugänglich machen.

Konfiguration mit Weboberfläche

Um das **Portforwarding** zu **aktivieren**, aktivieren Sie im Menü „Dial-Out“ auf der Seite „Portforwarding“ die Checkbox „Portforwarding für Dial-Out-Verbindungen aktivieren“.

Um eine **Regel für eine Weiterleitung** zu **erstellen**, wählen Sie das Protokoll (TCP oder UDP), den Bereich der Ports für die am MoRoS UMTS PRO 2.0 eingehenden Pakete. Geben Sie eine IP-Adresse für das Umleitungsziel im Eingabefeld „an IP-Adresse“ und einen Port im Eingabefeld „an Port“ ein; an diese Adresse und diesen Port werden die Pakete weitergeleitet. Klicken Sie anschließend auf „OK“, um die Regel zu speichern.

Um eine **bereits erstellte Regel** zu **deaktivieren**, deaktivieren Sie die Checkbox „aktiv“ und klicken Sie anschließend auf „OK“.

Um eine **bereits erstellte Regel** zu **löschen**, aktivieren Sie die Checkbox „löschen“ und klicken Sie anschließend auf „OK“.

Die Regeln in der Liste werden von oben nach unten abgearbeitet. Sollten sich also zwei Regeln widersprechen (z.B. zweimal derselbe Port), so wird nur die Regel ausgeführt, die weiter oben in der Liste steht.

12.4.8 Exposed Host festlegen

Optional kann der MoRoS UMTS PRO 2.0 alle Pakete, die keiner Portforwarding-Regel entsprechen, an einen vorbestimmten Rechner im LAN, den „Exposed Host“ weiterleiten (z.B. zu Diagnosezwecken). Die Einstellung für den „Exposed Host“ ist im Prinzip eine Portforwarding-Regel ohne Kriterien, die deshalb für alle Pakete gilt. Der „Exposed Host“ erhält alle Pakete, die nicht aus dem lokalen Netz des MoRoS UMTS PRO 2.0 angefordert wurden oder durch eine Portforwarding-Regel nicht bereits an einen Teilnehmer im lokalen Netz weitergeleitet wurden. Wird kein „Exposed Host“ konfiguriert, werden diese eingehenden Pakete verworfen.

Konfiguration mit Weboberfläche

Um einen **„Exposed Host“** zu **definieren**, geben Sie im Menü „Dial-Out“ auf der Seite „Portforwarding“ im Eingabefeld „Exposed Host“ die IP-Adresse eines Rechners im LAN ein, der von außen über alle Ports erreichbar sein soll.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.5 VPN

12.5.1 VPN Allgemein

Ein VPN (virtuelles privates Netzwerk) wird eingesetzt, um IP-Endgeräte oder ganze Netzwerke gesichert miteinander zu verbinden. Daten werden damit fälschungssicher an ein Ziel übertragen und sind für Dritte nicht lesbar.

Sie können den MoRoS UMTS PRO 2.0 als OpenVPN-Server oder als OpenVPN-Client nutzen. Dies ist von der Art des Verbindungsaufbaus (Dial-In oder Dial-Out) unabhängig.

Abbildung 6 zeigt eine Beispielkonfiguration für ein VPN. Hier ist ein MoRoS UMTS PRO 2.0 als OpenVPN-Server und ein zweiter MoRoS UMTS PRO 2.0 als OpenVPN-Client konfiguriert. Client als auch Server können durch beliebige OpenVPN-fähige Geräte ersetzt werden. Im Beispiel besteht eine PPP-Verbindung zwischen den beiden Geräten. Über diese PPP-Verbindung ist eine OpenVPN-Verbindung aufgebaut.

Sobald über die Funktion Dial-In oder Dial-Out eine PPP-Verbindung aufgebaut wurde können IP-Verbindungen zwischen den beiden Netzwerken aufgebaut werden. OpenVPN nutzt eine vorhandene PPP-Verbindung, um einen VPN Tunnel innerhalb dieser PPP-Verbindung aufzubauen. Dieser Tunnel besteht aus einer einzigen IP-Verbindung. OpenVPN stellt für den Datenverkehr eine virtuelle Netzwerkkarte zur Verfügung, über die dann der verschlüsselte Datenverkehr gesendet wird.

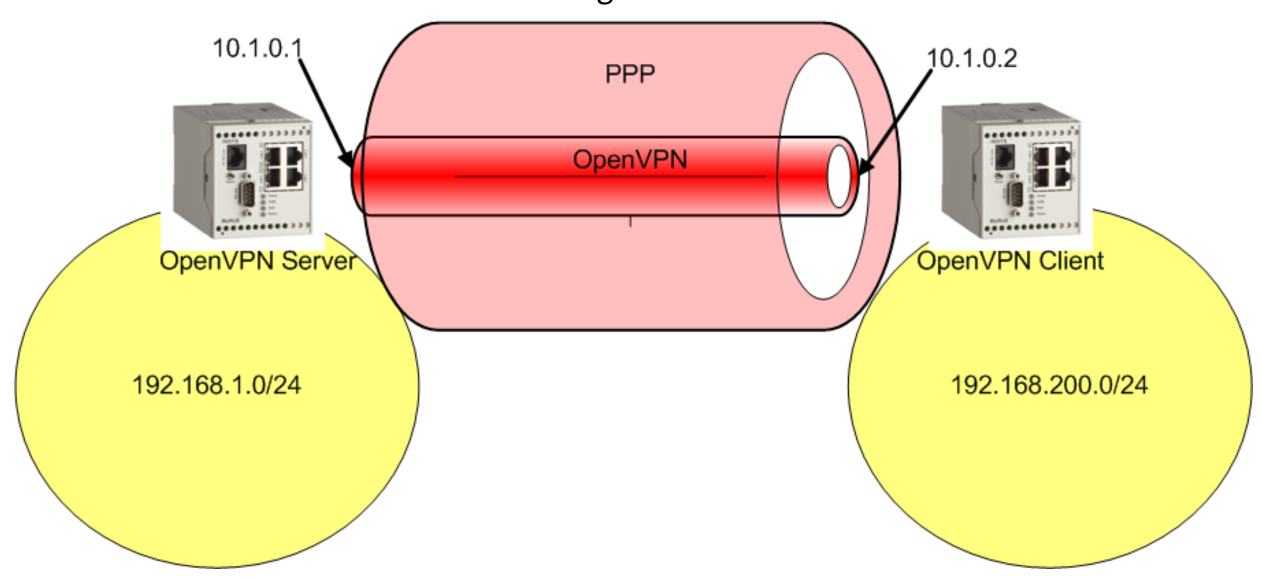


Abbildung 6: OpenVPN-Netz und IP Adressen in der Beispielkonfiguration

In der Beispielkonfiguration haben die Endpunkte der OpenVPN-Verbindung die IP-Adressen 10.1.0.1 und 10.1.0.2. Der VPN-Tunnel wird innerhalb einer schon bestehenden PPP-Verbindung aufgebaut. Den OpenVPN-Clients und Servern muss auch bekannt sein welches Netzwerk sich hinter dem jeweiligen Ende des VPN-Tunnels befindet. Die Netzwerke hinter den Enden sind die Zielnetze in die Daten gesendet werden sollen. In der Beispielkonfiguration ist das auf der einen Seite das Netzwerk 192.168.200.0/24. Auf der anderen Seite ist dies das Netzwerk 192.168.1.0/24. Sobald der Tunnel aufgebaut ist, werden Daten für diese Zielnetze durch den OpenVPN-Tunnel übertragen. Soll der komplette Datenverkehr aus einem Netz hinter dem MoRoS UMTS PRO 2.0 über den VPN-Tunnel geleitet werden, empfiehlt es sich, nach erfolgreicher Konfiguration die Firewall zu aktivieren. Damit kann die Kommunikation auf den Port beschränkt werden, über den der OpenVPN-Tunnel aufgebaut wird (Standardeinstellung Port 1194).

Der MoRoS UMTS PRO 2.0 unterstützt verschiedene Authentifizierungsmethoden beim Aufbau des VPN-Tunnels:

Authentifizierungsart	Verwendung	Besonderheit
Keine	Zu Testzwecken und zum Verbinden von Netzwerken ohne Verschlüsselung.	Keine verschlüsselte Verbindung. Am Server können sich nicht mehrere Clients gleichzeitig anmelden.
Statischer Schlüssel	Zum verschlüsselten Verbinden von je einem Client und Server in kleineren Anwendungen	Verschlüsselte Verbindung. Am Server können sich nicht mehrere Clients gleichzeitig anmelden.
Benutzername/Passwort und gemeinsames CA-Zertifikat (nur beim OpenVPN-Client einstellbar)	Zum verschlüsselten Verbinden von einem oder mehreren Clients zu einem OpenVPN-Server.	Flexible Anwendung für mehrere Clients.
Zertifikatsbasiert, jeder Teilnehmer hat ein individuelles Zertifikat und Schlüssel.	Zum verschlüsselten Verbinden von einem oder mehreren Clients zu einem OpenVPN-Server.	Lösung für maximale Sicherheit, allerdings etwas aufwändiger zu konfigurieren.

Tabelle 11: Authentifizierungsmethoden bei OpenVPN

Für detaillierte Informationen und Troubleshooting empfehlen wir auch die Webseite von OpenVPN: **http://openvpn.net/howto.html**

12.5.2 OpenVPN-Server Grundeinstellungen

Sie können den MoRoS UMTS PRO 2.0 als VPN-Server nutzen, wenn Sie z.B. vertrauliche Daten über ein unsicheres Netzwerk übertragen wollen. Dieser Abschnitt beschreibt die VPN-Server Grundeinstellungen. Die Grundeinstellungen sind beim MoRoS UMTS PRO 2.0 ab Werk auf sinnvolle Standardwerte gesetzt, die Sie aber unter besonderen Umständen abändern können. Mit den VPN-Grundeinstellungen legen Sie fest, über welchen Port der MoRoS UMTS PRO 2.0 den VPN-Tunnel erzeugt und ob die VPN-Übertragung mit dem UDP oder TCP-Protokoll umgesetzt wird. Weiterhin legen Sie hier fest, ob LZO-Komprimierung verwendet wird, welcher Verschlüsselungsalgorithmus während der Übertragung verwendet wird, wie groß die Tunnelpakete sein sollen und in welchen Zeitintervallen der VPN-Server VPN-Pings verschickt. Zusätzlich haben Sie hier die Möglichkeit, den OpenVPN-Status, die momentane Konfigurationsdatei anzuzeigen, eine Konfiguration für eine OpenVPN-Gegenstelle zu erzeugen sowie ein Log der letzten Verbindung anzuzeigen. Die erzeugte Konfiguration können Sie z.B. zum Einrichten eines OpenVPN-Pakets auf einem Client-PC verwenden. Das OpenVPN-Paket für Windows-Clients können Sie auf der Webseite von INSYS MICROELECTRONICS herunterladen:

www.insys-tec.de/treiber

Dieses Programm dient als Gegenstelle, wenn Sie die OpenVPN-Verbindung zu einem Windows PC aufbauen wollen.

Konfiguration mit Weboberfläche

Um bei **einer Verbindung den OpenVPN-Server** zu verwenden, aktivieren Sie im Menü „Dial-In“ bzw. „Dial-Out“ auf der Seite „OpenVPN-Server“ die Checkbox „OpenVPN-Server starten“.

Um den **lokalen Port am MoRoS UMTS PRO 2.0 sowie den Port an der Gegenstelle festzulegen**, geben Sie in den Eingabefeldern „Tunneln über Port (lokal / Gegenstelle)“ einen Wert für die gewünschten Ports an (Voreinstellung 1194).

Das **Protokoll der VPN-Übertragung** wählen Sie mit den Radiobuttons „UDP“ oder „TCP“ aus. Es empfiehlt sich, UDP zu verwenden, um die Latenz gering zu halten.

Damit **entfernte VPN-Gegenstellen während einer Verbindung Ihre IP verändern können** („**Floating**“), aktivieren Sie die Checkbox „Gegenstelle darf Ihre IP-Adresse dynamisch ändern (float)“. Diese Einstellung ist standardmäßig aktiv.

Um die **LZO-Komprimierung an- oder abzuschalten**, aktiveren oder deaktivieren Sie die Checkbox „LZO-Komprimierung aktivieren“. Werden bereits stark komprimierte Daten (z.B. jpg) übertragen, hat die Komprimierung kaum Effekt, werden hingegen gut komprimierbare Daten (z.B. Text) übertragen, kann die Komprimierung eine deutliche Reduzierung des übertragenen Datenvolumens erreichen. Schalten Sie die Kompression ab, falls Ihre Gegenstelle keine LZO-Kompression unterstützt.

Um eine **andere Verschlüsselungsmethode** als die voreingestellte „Blowfish 128 Bit“ für die VPN-Verbindung zu verwenden, wählen Sie im Dropdownmenü „Verschlüsselungsalgorithmus“ eine der folgenden Verschlüsselungsarten: (Blowfish 128 Bit), DES 64 Bit, DES EDE 128 Bit, DES EDE3 192 Bit, DESX 192 Bit, CAST5 128 Bit, IDEA 128 Bit, RC2 128 Bit, RC2 40 Bit, RC2 64 Bit, AES 128 Bit, AES 192 Bit, AES 256 Bit

Um die **Ausführlichkeit der Meldungen im Verbindungslog** einzustellen, geben Sie im Feld „Log-Level“ den Grad der Ausführlichkeit ein, wobei „0“ das Führen des Logs komplett deaktiviert und „9“ die meisten Details aufzeichnet.

Um eine bestimmte **Fragmentierungsgröße für die VPN-Tunnelpakte** in Bytes vorzugeben, verwenden Sie das Eingabefeld „Fragmentierung der Tunnelpakete“. Geben Sie hier die gewünschte maximale Paketgröße in Bytes an. Geben Sie hier keinen Wert an, haben die VPN-Pakete eine maximale Größe von 1500 Bytes. Die tatsächlich pro Paket übertragene Nutzdatenmenge ist geringer, da durch VPN ein „Protokoll-Overhead“ entsteht, d.h. die zu übertragenden Protokoll-Informationen verbrauchen einen Teil der Paketgröße.

Um das **Intervall bis zur Schlüsselerneuerung anzupassen**, verwenden Sie das Eingabefeld „Intervall bis zur Schlüsselerneuerung“. Geben Sie hier das Zeitintervall in Sekunden ein, nach dessen Ablauf neue Schlüssel erzeugt werden.

Um das VPN-Ping**-Intervall anzupassen**, verwenden Sie das Eingabefeld „Ping-Intervall“. Geben Sie hier das Zeitintervall in Sekunden ein, in dem der VPN-Server des MoRoS UMTS PRO 2.0 Ping-Pakete an die VPN-Gegenstelle versendet. Der regelmäßige Ping dient zum Offenhalten der Verbindung über diverse Router und Gateways, die evtl. an der Verbindung beteiligt sind und bei fehlender Kommunikation den Kanal schließen würden. Es empfiehlt sich hier ei-

nen Wert von einigen Minuten anzugeben, je nach benutztem Netzwerk und benutzter Infrastruktur.

Um das Ping-Restart**-Intervall anzupassen**, verwenden Sie das Eingabefeld „Ping-Restart-Intervall". Geben Sie hier ein, nach wie vielen Sekunden der Tunnel neu aufgebaut werden soll, wenn während der gesamten Zeit kein Ping von der Gegenstelle angekommen ist. Mit dem Wert „0" wird der Tunnel nie abgebaut, auch wenn kein Ping mehr empfangen.

12.5.3 OpenVPN-Server konfigurieren

Einrichten eines OpenVPN-Servers mit oder ohne Authentifizierung

Im Folgenden wird erklärt, wie Sie den MoRoS UMTS PRO 2.0 als VPN-Server einrichten können. Sie können den VPN-Server des MoRoS UMTS PRO 2.0 ohne Authentifizierung oder mit einer der beiden unterstützen Authentifizierungsmethoden (Zertifikatsbasiert oder per statischem Schlüssel) konfigurieren.

OpenVPN-Server mit zertifikatsbasierter Authentifizierung einrichten

Um einen OpenVPN-Server mit zertifikatsbasierter Authentifizierung einzurichten, müssen Sie zuerst Diffie-Hellman-Parameter, (CA-) Zertifikate und Schlüssel erzeugen. Danach können Sie mit den erzeugten Dateien den VPN-Server und die Clients einrichten. Die erzeugten Zertifikate und Schlüssel müssen dann auf den Server und die Clients entsprechend unten stehender Abbildung verteilt werden. Weiterhin ist es auch möglich, eine Certificate Revocation List auf den MoRoS UMTS PRO 2.0 zu laden. Für weitergehende Informationen zum Gebrauch und zur Erstellung von Zertifikaten empfehlen wir die Webseite von OpenVPN:
http://openvpn.net/howto.html

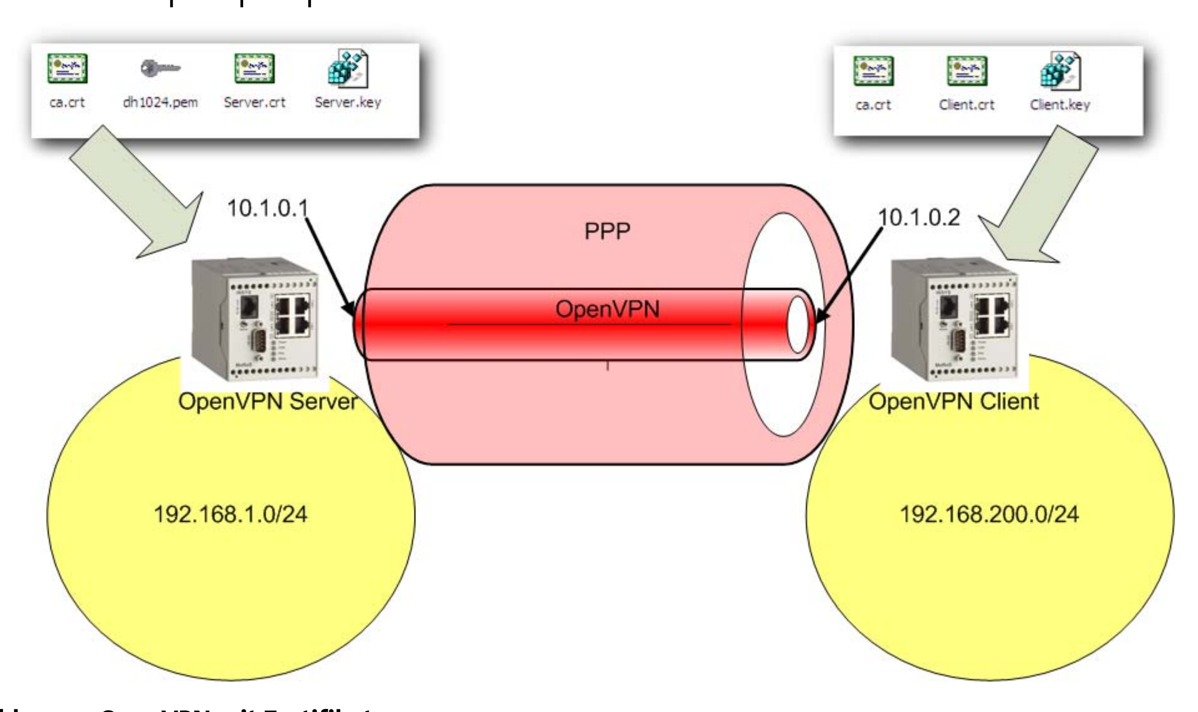


Abbildung 7: OpenVPN mit Zertifikaten

CA-Zertifikatsstruktur erzeugen (unter Windows)

So erzeugen Sie für den MoRoS UMTS PRO 2.0-VPN-Server sowie für die VPN-Clients eine CA-Zertifikatsstruktur, das auf alle Teilnehmer im OpenVPN-Netzwerk geladen werden muss.

⇢ Sie haben das OpenVPN-Paket (Version >=2.0.9) von der INSYS Homepage (www.insys-tec.de/treiber) heruntergeladen und installiert (wichtig sind die Installation der RSA-Skripte und eine SSL-Installation).

⇢ Die Uhrzeit des MoRoS UMTS PRO 2.0 ist korrekt eingestellt (Zertifikate haben ein Gültigkeitsdatum).

1. ***Öffnen Sie die MS-DOS-Eingabeaufforderung***

2. ***Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVP- Installation. (z.B. mit dem Befehl:*** `cd C:\Programme\OpenVPN\easy-rsa\`***)***

ⓘ Die Datei vars.bat kann editiert werden, um sie für Ihre Zwecke anzupassen (z.B. durch Anpassen der Vorgabewerte).

3. ***Führen Sie den Befehl*** `vars` ***aus***

✓ Eine Batch-Datei wird ausgeführt.

4. ***Führen Sie den Befehl*** `build-ca` ***aus.***

✓ Eine Batch-Datei wird ausgeführt. Der RSA-Schlüssel wird erzeugt.

✓ Sie finden im Unterverzeichnis „keys“ eine Datei mit dem Namen „ca.key“.

✓ Sie werden nun aufgefordert, den Ländercode einzugeben.

ⓘ Die folgenden Angaben dienen dazu, dass der Server identifiziert werden kann. Sie müssen bei allen Zertifikaten gleich sein.

5. ***Geben Sie den 2-Buchstaben-Code Ihres Landes an.***

ⓘ Geben Sie hier oder bei den folgenden Eingaben einen „ **.** “ ein, so wird das entsprechende Feld des Zertifikats leer gelassen.

6. ***Geben Sie den 2-Buchstaben-Code Ihrer Region an.***

ⓘ Die folgenden Eingaben können Sie auch in der Datei „vars.bat“ hinterlegen. So können Sie sich die wiederholte Eingabe ersparen.

7. ***Geben Sie den „Locality Name“ an, z.B. den Namen Ihrer Stadt.***

8. ***Geben Sie Ihren Firmennamen an.***

9. ***Geben Sie als „Common Name“ den Namen Ihres Servers (z.B. Hostname) an.***

ⓘ Dieses Feld dürfen Sie auf keinem Fall leer lassen. Mit dieser Angabe unterscheidet der Server später die verschiedenen Clients und Clientnetze.

10. ***Geben Sie die Email-Adresse an, die im Zertifikat hinterlegt werden soll.***

✓ Das CA-Zertifikat wird erzeugt. Sie finden im Unterverzeichnis „keys“ eine Datei mit dem Namen „ca.crt“.

Diffie-Hellman-Parameter erzeugen

So erzeugen Sie für den MoRoS UMTS PRO 2.0-VPN Server die Diffie-Hellman-Parameter. Ein Diffie-Hellmann-Parametersatz ist im Auslieferzustand bereits geladen, diesen Abschnitt können Sie also überspringen. Die Erzeugung der Parameter kann je nach Rechenleistung des PCs bis zu mehrere Minuten dauern. Diffie-Hellman-Parameter werden nur vom OpenVPN-Server benötigt, nicht von den Clients.

⇢ Sie haben das OpenVPN-Paket (Version >=2.0.9) von der INSYS Homepage heruntergeladen und installiert (www.insys-tec.de/treiber).

1. ***Öffnen Sie die MS-DOS-Eingabeaufforderung.***

2. ***Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVPN-Installation. (z.B. mit dem Befehl:*** `cd C:\Programme\OpenVPN\easy-rsa\`***)***

3. ***Führen Sie den Befehl*** `vars` ***aus.***

4. ***Geben Sie den Befehl*** `build-dh` ***ein.***

✓ Die Diffie-Hellmann-Parameter werden erzeugt

✓ Sie finden im Unterverzeichnis „keys“ eine Datei mit dem Namen „dh1024.pem“.

Private Key und Zertifikate für den Server und Clients erzeugen

So erzeugen Sie für den MoRoS UMTS PRO 2.0 VPN-Server sowie für die VPN-Clients die privaten Schlüssel und Zertifikate.

⇢ Sie haben das OpenVPN-Paket (Version >=2.0.9) von der INSYS Homepage heruntergeladen und installiert (www.insys-tec.de/treiber).

⇢ Sie haben bereits Diffie-Hellman-Parameter und ein CA-Zertifikatsstruktur erzeugt oder zur Verfügung.

1. ***Öffnen Sie die MS-DOS-Eingabeaufforderung.***

2. ***Wechseln Sie in das Verzeichnis „easy-rsa“ der OpenVPN-Installation. (z.B. mit dem Befehl:*** `cd C:\Programme\OpenVPN\easy-rsa\`***)***

3. ***Führen Sie den Befehl*** `vars` ***aus.***

ⓘ Der im Folgenden festgelegte Dateiname sollte keine Sonderzeichen enthalten. Der dann im Skript anzugebende „Common Name“ ist „Case Sensitive“ und sollte gleich dem Dateinamen sein.

4. ***Geben Sie den Befehl*** `build-key-server <file name>` ***ein. Geben Sie anstelle von <file name> Ihren Servernamen als Dateinamen ein z.B. „Server1“.***

✓ Das Skript fragt die zur Erstellung des Schlüssels notwendigen Informationen ab.

5. Beantworten Sie die Abfragen.

✓ Der Key und das Zertifikat werden erzeugt.

✓ Sie finden im Unterverzeichnis „keys“ zwei Dateien mit dem Namen „Server1.key“ und „Server1.crt“.

ⓘ Der im Folgenden festgelegte Dateiname sollte keine Sonderzeichen enthalten. Der dann im Skript anzugebende „Common Name“ ist „Case Sensitive“ und sollte gleich dem Dateinamen sein.

6. Geben Sie den Befehl `build-key <file name>` ein.
Geben Sie anstelle von <file name> Ihren Clientnamen als Dateinamen ein z.B. „Client“. Wiederholen Sie diesen Schritt für jeden einzelnen Client.

✓ Das Skript fragt die zur Erstellung des Schlüssels notwendigen Informationen ab.

7. Beantworten Sie die Abfragen.

✓ Der Client-Key und das Client-Zertifikat werden erzeugt.

✓ Sie finden im Unterverzeichnis „keys“ zwei Dateien mit dem Namen „Client.key“ und „Client.crt“ (für jeden Client).

✓ Die Erstellung der privaten Schlüssel und Zertifikate für OpenVPN-Server und die OpenVPN-Clients ist abgeschlossen.

Zertifikatsdateien und Schlüssel auf dem MoRoS UMTS PRO 2.0-OpenVPN-Server installieren und abschließend konfigurieren.

So richten Sie den MoRoS UMTS PRO 2.0-VPN Server mit den erzeugten Zertifikaten ein.

⇢ Sie haben bereits CA-Zertifikat, Diffie-Hellman-Parameter sowie private Schlüssel und Zertifikate für den Server sowie die Clients erzeugt.

1. Gehen Sie in der Webkonfiguration des MoRoS UMTS PRO 2.0 über den Menüpunkt „Dial-In“ bzw. „Dial-Out“ zur Seite „OpenVPN-Server“.

2. Wählen Sie den Radiobutton „Authentifizierung mit Zertifikaten“.

3. Klicken Sie auf OK , um die Einstellung zu speichern.

4. Klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf Durchsuchen.

5. ***Wählen Sie die Datei mit dem CA-Zertifikat (z.B. ca.crt) aus.***

6. ***Klicken Sie auf OK , um die Datei hochzuladen.***

7. ***Wiederholen Sie die Schritte 4-6 mit den Dateien „dh1024.pem“, „Server1.crt“ und „Server1.key“.***

✓ Bei „Diffie-Hellman-Parameter“ wird ein grüner Haken angezeigt, da diese bereits ab Werk geladen sind (sie können aber auch neu erzeugt werden).

✓ Anstelle des roten „X“ bei „CA-Zertifikat“ wird ein grüner Haken angezeigt.

✓ Anstelle des roten „X“ bei „Zertifikat“ wird ein grüner Haken angezeigt.

✓ Anstelle des roten „X“ bei „Privater Schlüssel“ wird ein grüner Haken angezeigt.

8. ***Geben Sie den Bereich der IP-Adressen für die Tunnelendpunkte der Clients im Eingabefeld „IP-Adressen-Pool für die Clients“ ein.***

ⓘ Aus diesem „Pool“ oder Netzwerk werden aufsteigend die Adressen für die Tunnelendpunkte der Clients vergeben.

9. ***Geben Sie eine Netzmaske für den Adresspool in das Eingabefeld „Netzmaske des IP-Adressen-Pools“ ein.***

10. ***Klicken Sie auf OK , um die Einstellungen zu speichern.***

11. ***Geben Sie unter „Neue Route zu Client-Netzwerk anlegen“ für jeden „Common Name“ der vergebenen Zertifikate die Adresse und die Netzmaske des Netzwerks hinter dem Tunnelende der Gegenstelle an. Speichern Sie jede Ihrer Eingaben mit einem Klick auf OK.***

ⓘ Die IP-Adresse eines Netzes ist in diesem Fall eine Adresse, die mit „0“ endet, z.B. 192.168.200.0. Die Netzmaske ist in diesem Fall 255.255.255.0. Mit dem Common Name aus dem Zertifikat werden die Routen zu den einzelnen Netzen unterschieden.

✓ Der MoRoS UMTS PRO 2.0-VPN-Server ist nun für die Verwendung der zertifikatsbasierten Authentifizierung vollständig konfiguriert.

ⓘ Damit Sie eine OpenVPN-Verbindung über den MoRoS UMTS PRO 2.0 aufbauen können, müssen Sie den OpenVPN-Server für Dial-In- bzw. Dial-Out-Verbindungen aktivieren.

OpenVPN-Server ohne Authentifizierung einrichten

Diesen Modus nutzen Sie für Testzwecke oder auch wenn Sie die Vorteile einer getunnelten IP-Verbindung nutzen wollen.

ⓘ Hierbei kann nur eine Verbindung zwischen einem Client und einem Server hergestellt werden.

⇢ Falls Sie einen PC als VPN-Gegenstelle verwenden: Sie haben das OpenVPN Paket (Version >=2.0.9) von der INSYS Homepage heruntergeladen und installiert (www.insys-tec.de/treiber).

1. Gehen Sie über den Menüpunkt „Dial-In“ bzw, „Dial-Out“ zur Seite „OpenVPN-Server“.

2. Wählen Sie den Radiobutton „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“.

3. Geben Sie die IP-Adresse oder den Domainnamen der Gegenstelle an, unter der die Gegenstelle im Internet erreichbar ist. An diese Adresse richtet sich der Verbindungsaufbau des VPN-Tunnels.

4. Geben Sie IP-Adressen für die Enden des VPN-Tunnels an.

ⓘ Die IP-Adressen der Tunnelenden müssen sich im gleichen Subnetz befinden.

ⓘ An der VPN-Gegenstelle müssen Sie diese Tunneladressen vertauschen, d.h. die Adresse, die am Server das lokale Tunnelende darstellt, ist von der Gegenstelle aus betrachtet „remote“ bzw. das entfernte Tunnelende.

5. Geben Sie die Netzwerkadresse und die Netzmaske des Netzwerks hinter den Tunnelende der Gegenstelle an.

ⓘ Die IP-Adresse eines Netzes ist in diesem Fall eine Adresse, die mit „0“ endet, z.B. 192.168.200.0. Die Netzmaske ist in diesem Fall 255.255.255.0.

6. Klicken Sie auf OK , um Ihre Einstellungen zu speichern.

✓ Der VPN-Server ist nun für eine VPN-Verbindung ohne Authentifizierung konfiguriert.

7. Konfigurieren Sie die VPN-Gegenstelle entsprechend Ihrer VPN-Serverkonfiguration.

ⓘ Verwenden Sie zum Konfigurieren der VPN-Gegenstelle die Funktion „Beispielkonfigurationsdatei für die Gegenstelle erstellen“.

ⓘ Damit Sie eine OpenVPN-Verbindung über den MoRoS UMTS PRO 2.0 aufbauen können, müssen Sie den OpenVPN-Server für Dial-In- bzw. Dial-Out-Verbindungen aktivieren.

OpenVPN-Server mit statischem Schlüssel einrichten

So richten Sie den MoRoS UMTS PRO 2.0-VPN Server mit Authentifizierung über einen statischen Schlüssel ein. Dies ist für kleinere Anwendungen sinnvoll, bei denen der Aufwand für Zertifikatserstellung und -verwaltung übertrieben wäre.

⇢ Falls Sie einen PC als VPN-Gegenstelle verwenden: Sie haben das OpenVPN Paket (Version >=2.0.9) von der INSYS Homepage heruntergeladen und installiert (www.insys-tec.de/treiber)

1. Gehen Sie über den Menüpunkt „Dial-In“ bzw, „Dial-Out“ zur Seite „OpenVPN-Server“.

2. Wählen Sie den Radiobutton „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“.

3. Klicken Sie auf „Statischen Schlüssel neu erstellen.

➢ *Alternativ können Sie einen schon vorhandenen Schlüssel hochladen. Klicken Sie hierzu im Abschnitt „Schlüssel oder Zertifikate laden“ auf „Durchsuchen“, wählen Sie eine Schlüsseldatei aus und klicken Sie anschließend auf die Schaltfläche „OK“, um die Datei auf den MoRoS UMTS PRO 2.0 zu laden.*

✓ Die Seite wird neu aufgebaut. Hinter dem Hinweis „Statischer Schlüssel vorhanden“ erscheint ein Link zum Herunterladen des statischen Schlüssels (sowie ein Link zum Löschen dieses Schlüssels).

4. Laden Sie sich den Schlüssel zum späteren Konfigurieren der Gegenstelle herunter, da der Server und der Client denselben Schlüssel benutzen müssen.

5. Geben Sie die IP-Adresse oder den Domainnamen der Gegenstelle an.

➢ *Alternativ können Sie die Datei vars.bat mit sinnvollen Voreinstellungen versehen. Dies erspart Ihnen wiederkehrende Eingaben.*

ⓘ An diese Adresse richtet sich der Verbindungsaufbau des VPN-Tunnels.

6. Geben Sie IP-Adressen für die Enden des VPN-Tunnels an.

ⓘ Die IP-Adressen der Tunnelenden müssen sich im gleichen Subnetz befinden.

ⓘ An der VPN-Gegenstelle müssen Sie diese Tunneladressen vertauschen, d.h. die Adresse, die am Server das lokale Tunnelende darstellt, ist von der Gegenstelle aus betrachtet „remote“ bzw. das entfernte Tunnelende.

7. Geben Sie die Netzwerkadresse und die Netzmaske des Netzwerks hinter dem Tunnelende der Gegenstelle an.

ⓘ Die IP-Adresse eines Netzes ist in diesem Fall eine Adresse, die mit „0“ endet, z.B. 192.168.200.0. Die Netzmaske ist in diesem Fall 255.255.255.0.

8. Klicken Sie auf OK , um Ihre Einstellungen zu speichern.

✓ Der VPN-Server ist nun für eine VPN-Verbindung mit Authentifizierung über einen statischen Schlüssel konfiguriert.

9. Konfigurieren Sie die VPN-Gegenstelle entsprechend Ihrer VPN-Serverkonfiguration.

ⓘ Verwenden Sie zum Konfigurieren der VPN-Gegenstelle die Funktion „Beispielkonfigurationsdatei für die Gegenstelle erstellen“.

ⓘ Damit Sie eine OpenVPN-Verbindung über den MoRoS UMTS PRO 2.0 aufbauen können, müssen Sie den OpenVPN-Server für Dial-In- bzw. Dial-Out-Verbindungen aktivieren.

12.5.4 OpenVPN-Client Grundeinstellungen

Sie können den MoRoS UMTS PRO 2.0 als VPN-Client nutzen, um sich mit einem VPN-Server über ein unsicheres Netz zu verbinden. Dieser Abschnitt beschreibt die VPN-Client Grundeinstellungen. Die Grundeinstellungen sind beim MoRoS UMTS PRO 2.0 ab Werk auf sinnvolle Standardwerte gesetzt, die Sie aber an das VPN anpassen müssen, mit dem sich der MoRoS UMTS PRO 2.0 verbinden soll. Mit den VPN-Grundeinstellungen legen Sie fest, mit welcher IP-Adresse oder Domain und über welche Ports der VPN-Tunnel aufgebaut wird, und ob die VPN-Übertragung mit dem UDP- oder TCP-Protokoll umgesetzt wird. Weiterhin legen Sie hier fest, ob LZO-Komprimierung verwendet wird, welcher Verschlüsselungsalgorithmus während der Übertragung verwendet wird, wie groß die Tunnelpakete sein sollen und in welchen Zeitintervallen der MoRoS UMTS PRO 2.0-OpenVPN-Client VPN-Pings an den Server verschickt. Zusätzlich haben Sie hier die Möglichkeit, den OpenVPN-Status, die momentane Konfigurationsdatei, eine Konfiguration für eine OpenVPN-Gegenstelle (den OpenVPN-Server) und ein Log der letzten Verbindung anzuzeigen.

Konfiguration mit Weboberfläche

Um bei **einer Verbindung den OpenVPN-Client** zu verwenden, aktivieren Sie im Menü „Dial-In“ bzw. „DIal-Out“ auf der Seite „OpenVPN-Client“ die Checkbox „OpenVPN-Client starten“.

Um die **IP-Adresse oder den Domainnamen der Gegenstelle zu bestimmen**, mit dem Sie den MoRoS UMTS PRO 2.0 die VPN-Verbindung aufbauen lassen, geben Sie im Feld „IP-Adresse oder Domainname der Gegenstelle“ eine IP-Adresse oder einen Domainnamen an.

Optional kann eine **alternative Gegenstelle bestimmt werden**, mit der der MoRoS UMTS PRO 2.0 die VPN-Verbindung aufbauen soll, falls die oben konfigurierte Gegenstelle nicht erreichbar ist. Geben Sie dazu im Feld „Alternative Gegenstelle“ eine IP-Adresse oder einen Domainnamen an.

Um den **lokalen Port am MoRoS UMTS PRO 2.0 sowie den Port an der Gegenstelle festzulegen**, geben Sie in den Eingabefeldern „Tunneln über Port (lokal / Gegenstelle)“ einen Wert für die gewünschten Ports an.

Das **Protokoll der VPN-Übertragung** wählen Sie mit den Radiobuttons „UDP" oder „TCP" aus. Wir empfehlen, UDP zu verwenden, um die Latenz gering zu halten.

Es ist nicht zwingend nötig, den **lokalen Port und die IP-Adresse der OpenVPN Verbindung** fest vorzuschreiben. Wenn Sie die Verwendung des Ports und der IP-Adresse offen lassen wollen, deaktivieren Sie die Checkbox „Lokale Adresse und Port fixieren (nobind)".

Damit **entfernte VPN-Gegenstellen Ihre IP-Adresse verändern können** („**Floating**"), aktivieren Sie die Checkbox „Gegenstelle darf Ihre IP-Adresse dynamisch ändern (float)". Diese Einstellung ist standardmäßig aktiv.

Um die **LZO-Komprimierung an- oder abzuschalten**, aktiveren oder deaktivieren Sie die Checkbox „LZO-Komprimierung aktivieren". Werden bereits stark komprimierte Daten (z.B. jpg) übertragen, hat die Komprimierung kaum Effekt, werden hingegen gut komprimierbare Daten (z.B. Text) übertragen, kann die Komprimierung eine deutliche Reduzierung des übertragenen Datenvolumens erreichen. Schalten Sie die Kompression ab, falls Ihre Gegenstelle keine LZO-Kompression unterstützt.

Um eine **andere Verschlüsselungsmethode** als die voreingestellte „Blowfish 128 Bit" für die VPN-Verbindung zu verwenden, wählen Sie im Dropdownmenü „Verschlüsselungsalgorithmus" eine der folgenden Verschlüsselungsarten:
(Blowfish 128 Bit), DES 64 Bit, DES EDE 128 Bit, DES EDE3 192 Bit,
DESX 192 Bit, CAST5 128 Bit, IDEA 128 Bit, RC2 128 Bit, RC2 40 Bit, RC2 64 Bit,
AES 128 Bit, AES 192 Bit, AES 256 Bit

Um die eine bestimmte **Fragmentierungsgröße für die VPN-Tunnelpakte** in Bytes vorgeben, verwenden Sie das Eingabefeld „Fragmentierung der Tunnelpakete". Geben Sie hier die gewünschte Paketgröße in Bytes an. Geben Sie hier keinen Wert an, haben die VPN-Pakete eine maximale Größe von 1500 Bytes. Die tatsächlich pro Paket übertragene Nutzdatenmenge ist geringer, da durch VPN ein „Protokoll-Overhead" entsteht, d.h. die zu übertragenden Protokoll-Informationen verbrauchen einen Teil der Paketgröße.

Um das **VPN-Ping-Intervall anzupassen**, verwenden Sie das Eingabefeld „Ping-Intervall". Geben Sie hier das Zeitintervall in Sekunden ein, in dem der VPN-Client des MoRoS UMTS PRO 2.0 Ping-Pakete an die VPN-Gegenstelle versendet. Der regelmäßige Ping dient zum Offenhalten der Verbindung über diverse Router und Gateways, die evtl. an der Verbindung beteiligt sind und bei fehlender Kommunikation den Kanal schließen würden.

Sie können die **Zeit** definieren, nach der die **VPN-Verbindung neu aufgebaut** wird, wenn ein Ping-Paket nicht beantwortet wird. Stellen Sie dafür eine Zeit in Sekunden im Eingabefeld „Ping-Restart-Intervall" ein.

Um zusätzlich einen **Ping per ICMP-Protokoll** an eine Domain oder eine IPAdresse zu senden, geben Sie diese in das Eingabefeld „Zusätzlicher ICMP-Ping an" ein. Es empfiehlt sich, hier einen Domainnamen oder eine IP-Adresse einzutragen, die nur durch den Tunnel erreichbar ist. Ist der Ping nicht erfolgreich, wird ein eventuell bestehender Tunnel abgebaut und ein neuer Tunnel aufgebaut. Das Intervall der Pings beträgt 15 Minuten.

12.5.5 OpenVPN-Client konfigurieren

Einrichten des OpenVPN-Client mit oder ohne Authentifizierung

Im Folgenden wird erklärt, wie Sie den MoRoS UMTS PRO 2.0 als VPN-Client einrichten können. Sie können den VPN-Client des MoRoS UMTS PRO 2.0 ohne Authentifizierung oder mit einer der beiden unterstützen Authentifizierungsmethoden (Zertifikatsbasiert oder per statischem Schlüssel) konfigurieren.

OpenVPN-Client mit CA-Zertifikat und Benutzername / Passwort einrichten

So richten Sie den MoRoS UMTS PRO 2.0-VPN Client für die Authentifizierung mit Benutzername und Passwort ein. Diese Authentifizierungsart verwendet Zertifikate, allerdings hat hier nicht jeder VPN-Teilnehmer ein eigenes Zertifikat.

⇢ Sie besitzen ein CA-Zertifikat für Ihr VPN.

⇢ Sie besitzen einen Benutzernamen und ein Passwort für die Authentifizierung an der OpenVPN-Gegenstelle.

1. ***Gehen Sie über den Menüpunkt „Dial-In“ bzw. „Dial-Out“ zur Seite „OpenVPN-Client“.***
2. ***Wählen Sie den Radiobutton „Authentifizierung mit Zertifikaten“.***
3. ***Klicken Sie auf OK , um die Einstellung zu speichern.***
4. ***Klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf Durchsuchen.***
5. ***Wählen Sie eine Datei mit der Endung „.crt“ mit dem CA-Zertifikat für Ihr VPN aus.***
6. ***Klicken Sie auf OK , um die Zertifikatsdatei auf den MoRoS UMTS PRO 2.0 zu laden.***

✓ Die Seite wird neu aufgebaut. Es erscheint ein grüner Haken anstelle des roten „X“ links neben dem Text „CA-Zertifikat vorhanden“.

7. ***Stellen Sie sicher, das die IP-Adresse oder der Domainname der Gegenstelle eingestellt ist.***

ⓘ An diese Adresse richtet sich der Verbindungsaufbau des VPN-Tunnels.

8. ***Geben Sie Benutzername und Passwort zur Authentifizierung bei der VPN-Gegenstelle an.***

➢ *Aktivieren Sie ggf. die Checkbox „Zertifikatstyp der Gegenstelle prüfen“, damit sich die Gegenstelle mit Ihrem Serverzertifikat als echter Server ausweist. So schränken Sie die Gefahr eines „Man-In-The-Middle“-Angriffs auf Ihr VPN stark ein.*

9. ***Klicken Sie auf OK , um Ihre Einstellungen zu speichern.***

✓ Der OpenVPN-Client ist nun für eine VPN-Verbindung mit CA-Zertifikat und Benutzername / Passwort konfiguriert.

ⓘ Damit Sie eine OpenVPN-Verbindung über den MoRoS UMTS PRO 2.0 aufbauen können, müssen Sie den OpenVPN-Client für Dial-In- bzw. Dial-Out-Verbindungen aktivieren.

OpenVPN-Client für zertifikatsbasierte Authentifizierung konfigurieren

So richten Sie den MoRoS UMTS PRO 2.0-VPN Client für die zertifikatsbasierte Authentifizierung ein.

⇢ Sie haben einen für Ihr VPN passendes CA-Zertifikat, sowie einen privaten Schlüssel und ein Zertifikat von der VPN-Administration erhalten oder selbst erzeugt.

1. ***Gehen Sie in der Webkonfiguration des MoRoS UMTS PRO 2.0 über den Menüpunkt „Dial-In“ bzw. „Dial-Out“ zur Seite „OpenVPN-Client“.***

2. ***Klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf Durchsuchen.***

3. ***Wählen Sie die Datei mit dem CA-Zertifikat (z.B. ca.crt) aus.***

4. ***Klicken Sie auf OK , um die Datei auf den MoRoS UMTS PRO 2.0 zu laden.***

5. ***Wiederholen Sie die Schritte 2-4 mit den Dateien „<Ihr_Zertifikat>.crt“ und „<Ihr_Schlüssel>.key“.***

✓ Anstelle des roten „X“ bei „CA-Zertifikat“ wird ein grüner Haken angezeigt.

✓ Anstelle des roten „X“ bei „Zertifikat“ wird ein grüner Haken angezeigt.

✓ Anstelle des roten „X“ bei „Privater Schlüssel“ wird ein grüner Haken angezeigt.

ⓘ Wenn noch ein rotes Kreuz vorhanden ist, erfolgt keine Authentifizierung mit Zertifikaten. Wenn ein Benutzername mit Kennwort vergeben wurde, wird ausschließlich dies zur Authentifizierung verwendet. Wenn alle Einträge mit grünen Haken versehen sind, werden Zertifikate zur Authentifizierung verwendet. Wenn dazu auch noch ein Benutzername mit Kennwort vergeben wurde, wird dies zusätzlich zu den Zertifikaten zur Authentifizierung verwendet.

➢ *Aktivieren Sie ggf. die Checkbox „Zertifikatstyp der Gegenstelle prüfen“, damit sich die Gegenstelle mit Ihrem Serverzertifikat als echter Server ausweist. So schränken Sie die Gefahr eines „Man-In-The-Middle“-Angriffs auf Ihr VPN stark ein.*

6. ***Klicken Sie auf OK , um die Einstellungen zu speichern.***

7. ***Stellen Sie sicher, das die IP-Adresse oder der Domainname der Gegenstelle eingestellt ist.***

✓ Der MoRoS UMTS PRO 2.0-OpenVPN-Client ist nun für die Verwendung der zertifikatsbasierten Authentifizierung vollständig konfiguriert.

ⓘ Damit Sie eine OpenVPN-Verbindung über den MoRoS UMTS PRO 2.0 aufbauen können, müssen Sie den OpenVPN-Client für Dial-In- bzw. Dial-Out-Verbindungen aktivieren.

OpenVPN-Client ohne Authentifizierung einrichten

So richten Sie den MoRoS UMTS PRO 2.0-VPN Client ohne Verwendung einer Authentifizierungsmethode ein. Dies ist für Testzwecke sinnvoll oder wenn Sie die Vorteile einer getunnelten IP-Verbindung nutzen wollen.

ⓘ Hierbei kann nur eine Verbindung zwischen einem Client und einem Server hergestellt werden.

→ Sie benötigen keine verschlüsselte Übertragung.

1. ***Gehen Sie über den Menüpunkt „Dial-In“ bzw. „Dial-Out“ zur Seite „OpenVPN-Client“.***

2. ***Wählen Sie den Radiobutton „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“.***

3. ***Stellen Sie sicher, das die IP-Adresse oder der Domainname der Gegenstelle eingestellt ist.***

ⓘ An diese Adresse richtet sich der Verbindungsaufbau des VPN-Tunnels.

4. ***Geben Sie IP-Adressen für die Enden des VPN-Tunnels an.***

ⓘ Die IP-Adressen der Tunnelenden müssen sich im gleichen Subnetz befinden.

ⓘ An der VPN-Gegenstelle des Servers müssen diese Tunneladressen „spiegelverkehrt“ eingetragen sein, d.h die Adresse, die am Server das lokale Tunnelende darstellt, ist von der Client aus betrachtet „remote“ bzw. das entfernte Tunnelende und umgekehrt.

5. ***Geben Sie die Netzwerkadresse und die Netzmaske des Netzwerks hinter dem Tunnelende der Gegenstelle an.***

ⓘ Die IP-Adresse eines Netzes ist in diesem Fall eine Adresse, die mit „0“ endet, z.B. 192.168.200.0. Die Netzmaske ist in diesem Fall 255.255.255.0.

6. ***Klicken Sie auf OK , um Ihre Einstellungen zu speichern.***

✓ Der VPN-Client ist nun für eine VPN-Verbindung ohne Authentifizierung konfiguriert.

ⓘ Damit Sie eine OpenVPN-Verbindung über den MoRoS UMTS PRO 2.0 aufbauen können, müssen Sie den OpenVPN-Client für Dial-In- bzw. Dial-Out-Verbindungen aktivieren.

OpenVPN Client mit statischem Schlüssel einrichten

So richten Sie den MoRoS UMTS PRO 2.0-VPN Client mit Authentifizierung über einen statischen Schlüssel ein. Dies ist für kleinere Anwendungen sinnvoll, bei denen der Aufwand für Zertifikatserstellung und -verwaltung nicht rentabel wäre.

→ Sie besitzen einen statischen Schlüssel für Ihr VPN (Sie können sich auch über das Webinterface des MoRoS UMTS PRO 2.0 einen statischen Schlüssel erstellen lassen).

1. ***Gehen Sie über den Menüpunkt „Dial-In“ bzw. „Dial-Out“ zur Seite „OpenVPN-Client“.***

2. ***Wählen Sie den Radiobutton „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“.***

3. ***Klicken Sie auf OK , um Ihre Einstellungen zu speichern.***

4. ***Klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf Durchsuchen.***

5. ***Wählen Sie die Datei .key mit dem Schlüssel für Ihr VPN aus.***

6. ***Klicken Sie auf OK , um die Schlüsseldatei hochzuladen.***

✓ Die Seite wird neu aufgebaut. Hinter dem Hinweis „Statischer Schlüssel vorhanden“ erscheint ein Link zum Herunterladen des statischen Schlüssels (sowie ein Link zum Löschen dieses Schlüssels).

7. ***Stellen Sie sicher, das die IP-Adresse oder der Domainname der Gegenstelle eingestellt ist.***

ⓘ An diese Adresse richtet sich der Verbindungsaufbau des VPN-Tunnels.

8. ***Geben Sie IP-Adressen für die Enden des VPN-Tunnels an.***

ⓘ Die IP-Adressen der Tunnelenden müssen sich im gleichen Subnetz befinden.

ⓘ An der VPN-Gegenstelle des Servers müssen diese Tunneladressen „spiegelverkehrt“ eingetragen sein, d.h. die Adresse, die am Server das lokale Tunnelende darstellt, ist von der Client aus betrachtet „remote“ bzw. das entfernte Tunnelende und umgekehrt

9. ***Geben Sie die Netzwerkadresse und die Netzmaske des Netzwerks hinter den Tunnelende der Gegenstelle an.***

ⓘ Die IP-Adresse eines Netzes ist in diesem Fall eine Adresse, die mit „0“ endet, z.B. 192.168.200.0. Die Netzmaske ist in diesem Fall 255.255.255.0.

10. ***Klicken Sie auf OK , um Ihre Einstellungen zu speichern.***

✓ Der OpenVPN-Client ist nun für eine VPN-Verbindung mit Authentifizierung über statische Schlüssel konfiguriert.

ⓘ Damit Sie eine OpenVPN-Verbindung über den MoRoS UMTS PRO 2.0 aufbauen können, müssen Sie den OpenVPN-Client für Dial-In- bzw. Dial-Out-Verbindungen aktivieren.

12.6 Redundantes Kommunikationsgerät

12.6.1 Redundantes Kommunikationsgerät einrichten

Sie können zur Erhöhung der Betriebssicherheit und Verfügbarkeit an den MoRoS UMTS PRO 2.0 ein zweites Kommunikationsgerät anschließen, um einen redundanten Übertragungsweg zur Verfügung zu halten. So kann bei einem Ausfall von einem Übertragungsweg (z.B. GSM) immer noch ein zweiter Übertragungsweg benutzt werden (z.B. Modem). Es sind beliebige Kombinationen aus Modem, ISDN und GSM/GPRS/EDGE/UMTS-Geräten möglich. Hierzu schließen Sie einfach ein weiteres INSYS Kommunikationsgerät über die serielle Schnittstelle des MoRoS UMTS PRO 2.0 an. Der MoRoS UMTS PRO 2.0 erkennt beim nächsten Systemstart automatisch, dass ein redundantes Übertragungsgerät zur Verfügung steht und ändert die Weboberfläche zur Konfiguration entsprechend ab.

Bitte wenden Sie sich an Ihren Vertriebspartner oder an INSYS Microelectronics um zu erfahren, welche weiteren INSYS Geräte sich für den Anschluss als redundantes Kommunikationsgerät eignen.

Sollte ein redundantes Kommunikationsgerät benutzt werden, kann die Funktion Seriell-Ethernet-Gateway nicht genutzt werden. Wird das Seriell-Ethernet-Gateway aktiviert, werden die Optionen für das redundante Kommunikationsgerät nicht angezeigt.

Konfiguration mit Weboberfläche

Wenn der MoRoS UMTS PRO 2.0 beim Systemstart ein redundantes Kommunikationsgerät an seiner seriellen Schnittstelle lokalisiert hat, stehen in den Menüs **Dial-In** und **Dial-Out weitere Auswahlmöglichkeiten** zur Verfügung.

Um den **Dial-In** für redundanten Betrieb zu **konfigurieren**, wählen Sie im Menü Dial-In aus, welches Kommunikationsgerät für Dial-In benutzt werden soll. Hier haben Sie die Möglichkeit, den Dial-In nur über eines der beiden Kommunikationsgeräte, über beide Kommunikationsgeräte oder gar nicht zu aktivieren.

Um den **Dial-Out** für redundanten Betrieb zu **konfigurieren**, wählen Sie im Menü Dial-Out aus, welches Kommunikationsgerät für Dial-Out benutzt werden soll. Hier haben Sie ebenfalls die Möglichkeit, den Dial-Out nur über eines der beiden Kommunikationsgeräte, über beide Kommunikationsgeräte oder gar nicht zu aktivieren. Hier können Sie außerdem festlegen, welches Kommunikationsgerät bevorzugt verwendet wird. Das zweite Kommunikationsgerät wird nur dann verwendet, wenn der Anwahlversuch über das erste Gerät nicht zum Erfolg geführt hat. Im Menü Dial-Out müssen Sie außerdem die Zielrufnummer und die Parameter für die PPP-Anwahl jeweils einzeln für die beiden Kommunikationsgeräte eintragen.

Speichern Sie Ihre Einstellungen, indem Sie jeweils auf „OK“ klicken.

12.7 Eingänge und Ausgänge

12.7.1 Status der Eingänge abfragen

Der MoRoS UMTS PRO 2.0 besitzt digitale Eingänge, die einen PPP-Verbindungsaufbau oder einen Nachrichtenversand per SMS auslösen können. Die Eingänge sind geschlossen, wenn sie mit GND verbunden sind. Sie sind geöffnet, wenn keine Verbindung mit GND besteht. Die Zustände der beiden Eingänge können Sie über die Weboberfläche abfragen.

Konfiguration mit Weboberfläche

Um den **Zustand der Eingänge abzufragen**, klicken Sie im Menü „Ein-Ausgänge“ auf der Seite „Eingänge“ auf die Schaltfläche „Aktualisieren“. Nach dem die Seite erneut geladen wurde, sehen Sie die Zustände der jeweiligen Eingänge neben „Eingang 1 :“ und „Eingang 2 :“.

12.7.2 Funktion der Eingänge konfigurieren

Der MoRoS UMTS PRO 2.0 kann beim Schließen des Eingangs 1 eine SMS an eine Rufnummer versenden und eine zuvor konfigurierte Dial-Out-Verbindung aufbauen, sobald der Eingang 2 für 4 Sekunden geschlossen, d.h. mit „GND“ verbunden, wird. Bei Aktivierung des Eingangs wird ein Dial-Out ausgeführt, wie er im Menü Dial-Out konfiguriert wurde. Die Verbindung bleibt solange bestehen, wie es die Verbindungskonfiguration zulässt.

Konfiguration mit Weboberfläche

Um die **Funktion von Eingang 1 zu konfigurieren**, wählen Sie im Menü „Ein-Ausgänge“ auf der Seite „Eingänge“ entweder die Option „keine“ oder „SMS-Versand bei Änderung aktivieren“.

Um die **Funktion von Eingang 2 zu konfigurieren**, wählen Sie im Menü „Ein-/Ausgänge“ auf der Seite „Eingänge“ entweder die Option „keine“, „Dial-Out-Verbindung auslösen“ oder „OpenVPN-Tunnel aufbauen“.
Die jeweiligen Funktionen Dial-Out bzw. VPN müssen konfiguriert sein, um vom Eingang geschaltet zu werden.

Um eine **Dial-Out-Verbindung nur durch Eingang 2 aufbauen zu lassen**, aktivieren Sie die Checkbox „Dial-Out-Verbindung exklusiv aufbauen (Dial-on-Demand nicht aktivieren)“.

Um eine **Dial-Out-Verbindung durch Öffnen von Eingang 2 abzubauen**, aktivieren Sie die Checkbox „Dial-Out-Verbindung beenden, wenn nicht mehr mit GND verbunden“.

Um einen **OpenVPN-Tunnel nur durch Eingang 2 aufbauen zu lassen**, aktivieren Sie die Checkbox „OpenVPN-Tunnel exklusiv über Eingang aufbauen (nicht automatisch nach Dial-Out)“.

Um einen **OpenVPN-Tunnel durch Öffnen von Eingang 2 abzubauen**, aktivieren Sie die Checkbox „OpenVPN-Tunnel abbauen, wenn nicht mehr mit GND verbunden“.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.7.3 SMS-Versand konfigurieren

Der MoRoS UMTS PRO 2.0 kann beim Schließen des Eingangs 1 eine SMS an eine Rufnummer versenden. Dabei wird zwischen einem langen, mindestens 4 Sekunden dauernden Puls und einzelnen Pulsen, die kürzer als 1 Sekunde andauern, unterschieden.

Der lange Puls löst die SMS-Nachricht für den einfachen Alarm aus. Die kurzen Pulse lösen den Versand der SMS-Nachrichten für die jeweilige Anzahl von Impulsen aus.

SMS-Nachrichten können bis zu 140 Zeichen lang sein.

Konfiguration mit Weboberfläche

Damit der SMS-Versand funktioniert, geben Sie im Menü „Ein-/Ausgänge“ auf der Seite „SMS-Versand“ die **Nummer eines SMS Service Centers** im Eingabefeld „SCN (Service Center Number) SIM-Karte 1“ an. Falls Sie eine zweite SIM-Karte verwenden, geben Sie die SMSC-Nummer für diese SIM-Karte im Eingabefeld „SCN (Service Center Number) SIM-Karte 2“ an.

Um **eine Nachricht durch** den einzelnen, **4 Sekunden andauernden Impuls** zu versenden, geben Sie bei „Einfacher Alarm“ eine Zielrufnummer im Eingabefeld „Rufnummer“ ein. Das Format der Zielrufnummer hängt von den Anforderungen des Service Centers ab. Erfragen Sie weitere Details über das Format der Zielrufnummer bei dem Betreiber Ihres Service Centers. Geben Sie den Text der SMS-Nachricht im zugehörigen Eingabefeld ein.

Um **eine Nachricht** für eine Anzahl von **kurzen, jeweils 1 Sekunde andauernden Impulsen** zu versenden, scrollen Sie im Menü „Ein-/Ausgänge“ auf der Seite „SMS-Versand“weiter nach unten bis zum Eingabefeld für die gewünschte Anzahl von Impulsen. Geben Sie bei der jeweiligen Anzahl der Pulse eine Zielrufnummer im Eingabefeld „Rufnummer“ an. Geben Sie den Text der SMS-Nachricht im zugehörigen Eingabefeld ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.7.4 Ausgänge schalten

Der MoRoS UMTS PRO 2.0 besitzt digitale Ausgänge, deren Status Sie über die Weboberfläche abfragen und ändern können.

Die Ausgänge können außerdem täglich zu einer bestimmten Uhrzeit betätigt werden. Weiterhin ist es möglich, die Ausgänge durch Aufbauen einer PPP- Verbindung bzw. eines OpenVPN-Tunnels zu betätigen.

Konfiguration mit Weboberfläche

Um den **Status der Ausgänge abzufragen**, wechseln Sie zum Menü „Ein-/Ausgänge" auf die Seite „Ausgänge". Der Status der Ausgänge wird im Abschnitt „Ausgänge manuell schalten" durch die Radiobuttons neben dem Text „Ausgang 1/2" angezeigt.

Um den **Zustand der Ausgänge umzuschalten**, wählen Sie im Menü „Ein-/Ausgänge" auf der Seite „Ausgänge" im Abschnitt „Ausgänge manuell schalten" über die Radiobuttons für den jeweiligen Ausgang „Ruhestellung" oder „Arbeitsstellung" aus, und klicken Sie auf „OK".

Um einen **Ausgang täglich zu einer bestimmten Zeit in Arbeitsstellung zu schalten**, aktivieren Sie im Abschnitt „Schaltzeiten Ausgang 1/2" die Checkbox „Arbeitsstellung um" und geben Sie dahinter die Uhrzeit ein, zu der der jeweilige Ausgang betätigt werden soll.

Um einen **Ausgang täglich zu einer bestimmten Zeit in Ruhestellung zu schalten**, aktivieren Sie im Abschnitt „Schaltzeiten Ausgang 1/2" die Checkbox „Ruhestellung um" und geben Sie dahinter die Uhrzeit ein, zu der der jeweilige Ausgang in Ruhestellung zurückkehren soll.

Um **Ausgang 1 für eine Betätigung bei Bestehen einer PPP-Verbindung zu konfigurieren**, wählen Sie unter „Funktion von Ausgang 1" die Option „schaltet auf Arbeitsstellung, wenn eine PPP-Verbindung besteht".

Um **Ausgang 2 für eine Betätigung bei Bestehen eines OpenVPN-Tunnels zu konfigurieren**, wählen Sie unter „Funktion von Ausgang 2" die Option „schaltet auf Arbeitsstellung, wenn ein OpenVPN-Tunnel besteht".

Übernehmen Sie die Einstellungen, indem Sie auf „OK" klicken.

12.8 Konfigurierbarer Switch

12.8.1 Konfiguration und Status der Switchports abfragen

Der Switch des MoRoS UMTS PRO 2.0 ist konfigurierbar. Das heißt, Sie können für jeden Switchport individuell bestimmen, welche Übertragungsrate verwendet oder ob er im Halb-duplex- oder Voll-duplex-Modus betrieben wird. Weiterhin können Sie über das Webinterface kontrollieren, an welchem Switchport ein Kabel angeschlossen ist und ob eine physische Verbindung besteht.

Konfiguration mit Weboberfläche

Die **momentane Konfiguration der einzelnen Switchports** sehen Sie im Menü „Switch" auf der Seite „Portkonfiguration" neben der Auflistung der Ports.

Ob ein Kabel am Switch angeschlossen ist, sehen Sie an den farbigen Kästchen. Diese Kästchen symbolisieren die vier Switchports. Die Kästchen sind grün, sobald ein Netzwerkkabel angeschlossen ist und rot, wenn kein Kabel angeschlossen ist bzw. keine physische Verbindung zum Netzwerk besteht.

12.8.2 Switchports konfigurieren

Sie können festlegen, welcher Switchport mit welcher Übertragungsrate betrieben wird und ob er halb-duplex oder voll-duplex betrieben wird. Weiterhin können Sie bestimmen, ob die Autonegotiation (die Erkennung der Netzwerkabelverdrahtung) am jeweiligen Port zur Verfügung steht. Diese Einstellungen können nötig sein, falls Endgeräte Schwierigkeiten mit der automatischen Erkennung der Verbindungsparameter haben. Hier sollten also nur Einstellungen vorgenommen werden, wenn Verbindungsprobleme im lokalen Netzwerk mit einzelnen Geräten auftauchen.

Konfiguration mit Weboberfläche

Um den jeweiligen Switchport zu aktivieren oder deaktivieren, verwenden Sie im Menü „Switch" auf der Seite „Portkonfiguration" die Checkbox „aktiv" des jeweiligen Switchports.

Um die Autonegotiation an- oder abzuschalten, verwenden Sie im Menü „Switch" auf der Seite „Portkonfiguration" die Checkbox „Auto negotiation" des jeweiligen Switchports.

Um die Übertragungsrate eines Switchports festzulegen, verwenden Sie die Radiobuttons „10 Mbit/s" und „100 Mbit/s".

Um einen Switchport voll-duplex oder halb-duplex zu betreiben, verwenden Sie die Radiobuttons „Half Duplex" und „Full Duplex".

Speichern Sie Ihre Einstellungen, indem Sie auf „OK" klicken.

12.8.3 LED-Anzeige der Switchports konfigurieren

Sie können festlegen, wie die Ereignisse auf dem Netzwerk und die Zustände der Switchports and den Switchport-Status-LEDs angezeigt werden. Wir empfehlen, hier die Grundeinstellungen zu belassen und die Anzeigen nur kurzfristig für die Diagnose zu verändern.

Konfiguration mit Weboberfläche

Wählen Sie für das **jeweilige Netzwerkereignis oder den Zustand des Ports die Farbe der LED-Anzeige** der Switchport-Status-LED im Menü „Switch" auf der Seite „LED Konfiguration" über die Radiobuttons aus.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK" klicken.

12.8.4 Portspiegelung einrichten

Mit der Portspiegelung können Sie den Datenverkehr eines Switchports auf einen festlegbaren anderen Switchport, den Sniffer-Port kopieren. So ist es möglich, den Netzwerkverkehr für Analysezwecke mitzulesen. Es können hier getrennt die Sende und Empfangspakete (TX/RX) von bestimmten Ports auf einen Sniffer-Port gespiegelt werden, an dem dann der Netzwerkverkehr mitgelesen werden kann.

Konfiguration mit Weboberfläche

Um einen Port als Sniffer-Port zu verwenden, wählen Sie unter dem Menüpunkt „Switch" auf der Seite „Port spiegeln" im Dropdownmenü „Sniffer-Port" den entsprechenden Port aus.

Wählen Sie im Dropdownmenü „TX spiegeln an Sniffer-Port" den Port aus, **dessen Daten der TX-Leitung auf den Sniffer-Port kopiert** werden sollen.

Wählen Sie im Dropdownmenü „RX spiegeln an Sniffer-Port" **den Port aus, dessen Daten der RX-Leitung auf den Sniffer-Port kopiert** werden sollen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK" klicken.

12.9 Server-Dienste

12.9.1 DNS-Forwarding einrichten

Sie können den MoRoS UMTS PRO 2.0 als DNS-Relay-Server nutzen. Wenn der MoRoS UMTS PRO 2.0 bei den lokal angeschlossenen Netzwerkgeräten als DNS-Server konfiguriert wird, leitet der MoRoS UMTS PRO 2.0 die DNS-Abfragen entweder an die vorher konfigurierten DNS-Server im Internet weiter oder benutzt die beim PPP-Verbindungsaufbau übergebenen IP Adressen als DNS Server.

Konfiguration mit Weboberfläche

Dem MoRoS UMTS PRO 2.0 können beim PPP-Verbindungsaufbau DNS-Server übergeben werden. Damit der MoRoS UMTS PRO 2.0 die DNS-Abfragen an von Ihnen **bestimmte Name-Server** weiterleiten kann, geben Sie zusätzlich die Adressen der jeweiligen Nameserver in die Eingabefelder „Erste DNS-Server Adresse“ und „Zweite DNS-Server Adresse“ ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.9.2 Dynamisches DNS Update einrichten

Der MoRoS UMTS PRO 2.0 kann die IP-Adresse, die Ihm dynamisch bei der Interneteinwahl zugewiesen wurde, einem DynDNS-Provider mitteilen, um so aus dem Internet unter einem Domainnamen erreichbar zu sein. Damit ist das Netzwerk hinter dem MoRoS UMTS PRO 2.0 aus dem Internet auch bei dynamisch zugeteilten IP-Adressen immer unter demselben Domainnamen erreichbar (falls die zugewiesene IP-Adresse für eingehende Verbindungen nicht geschützt ist). Dafür aktualisiert der MoRoS UMTS PRO 2.0 bei jeder Einwahl die beim DynDNS-Provider mit dem Domainnamen verknüpfte IP-Adresse. Damit Sie diese Funktion nutzen können, benötigen Sie einen Account bei einem DynDNS-Provider.



Bei paketbasierten Wireless-Verbindungen (GPRS/EDGE/UMTS/HSDPA) muss auch eine öffentliche IP-Adresse vom Provider zugewiesen worden sein. Ansonsten ist das Gerät trotz dieses Dienstes nicht erreichbar.

Konfiguration mit Weboberfläche

Um das **dynamische DNS-Update einzurichten**, aktivieren Sie im Menü „Server-Dienste“ auf der Seite „Dyn. DNS-Update“ die Checkbox „Dynamisches DNS-Update aktivieren“.

Wählen Sie einen **DynDNS-Provider** aus dem Dropdown-Menü „DynDNS-Provider“.

Um **einen eigenen DynDNS-Server zu definieren**, wählen Sie im Dropdown-Menü „DynDNS-Provider“ den Eintrag „Userdefined DynDNS“ und geben Sie einen DynDNS-Server im Eingabefeld „Benutzerdefinierter DynDNS-Server“ an.

Geben Sie den zu **aktualisierenden Domainnamen** im Eingabefeld „Domainname“ ein.

Geben Sie den **Benutzernamen und das Passwort** Ihres DynDNS-Accounts in die Eingabefelder „Benutzername“ und „Kennwort“ ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.9.3 DHCP-Server einrichten

Der DHCP-Server des MoRoS UMTS PRO 2.0 kann auf Anfrage anderen Geräten im LAN automatisch eine Adresse zuweisen. Diese automatisch vergebenen, dynamischen IP-Adressen sind nur eine gewisse Zeit gültig. Die Gültigkeitsdauer der vom DHCP-Server vergebenen IP-Adressen steuern Sie über die „Lease Time“. Sollte sich im Netzwerk, in dem der MoRoS UMTS PRO 2.0 eingesetzt wird, bereits ein DHCP Server befinden, so muss diese Funktion im MoRoS UMTS PRO 2.0 unbedingt abgeschaltet werden.

IP-Adressen, die im IP-Pool liegen und für die eine Verknüpfung mit einer MAC-Adresse existiert, sind ausschließlich für diesen DHCP-Client reserviert. Die IP-Adresse liegt somit nicht mehr im IP-Pool. Es sollten für diese MAC-IP-Adress-Verknüpfungen keine IP-Adressen aus dem IP-Pool gewählt werden. Der Pool sollte nur für die DHCP-Clients zur Verfügung stehen, von denen keine MAC-Adresse bekannt ist oder berücksichtigt werden soll.

Konfiguration mit Weboberfläche

Um den **DHCP-Server** einzurichten, aktivieren Sie im Menü „Server-Dienste“ auf der Seite „DHCP“ die Checkbox „DHCP-Server aktivieren“.

Geben Sie in den Eingabefeldern „Erste und letzte IP-Adresse“ die **erste IP-Adresse** und die **letzte IP-Adresse** des Adressraumes ein, aus dem der DHCP-Server des MoRoS UMTS PRO 2.0 Adressen im LAN vergibt. Der IP-Adressraum des DHCP Servers muss in demselben Netzwerk liegen wie die IP-Adresse des MoRoS UMTS PRO 2.0.

Geben Sie im Eingabefeld „Lease Time“ eine **Gültigkeitsdauer** in Sekunden für die vom DHCP-Server zu vergebenden **IP-Adressen** ein. Der Standardwert ist 3600 Sekunden.

Um den **DHCP-Clients einen speziellen DNS-Server mitzuteilen**, geben Sie Eingabefeld „Alternative DNS-Server Adresse“ dessen Adresse ein. Ist das Feld leer, bekommen die Clients die lokale IP-Adresse des Routers und die IP-Adressen der fest eingestellten DNS-Server mitgeteilt.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

Um die vom DHCP-Server vergeben IP-Adressen sowie deren „Lease Time“ (Gültigkeitsdauer) einsehen, verwenden Sie den Link „DHCP-Lease Times anzeigen“.

Um bestimmten **DHCP-Clients immer die gleiche IP-Adresse zu geben**, können Sie im Abschnitt „Neue Zuordnung von MAC-Adresse und IP-Adresse“ feste Zuordnungen definieren. Geben Sie dazu in das Eingabefeld „MAC-Adresse“ die MAC-Adresse des jeweiligen DHCP-Clients und in das Feld „IP-Adresse“ die IP-Adresse, mit dem der DHCP-Client verknüpft werden soll, ein. Speichern Sie die Zuordnung, indem Sie auf „OK“ klicken.

Um **eine oder mehrere Zuordnungen** zu **löschen**, aktivieren Sie im Abschnitt „Feste Zuordnung von IP-Adressen zu MAC-Adressen“ die Checkbox in der Spalte „löschen“ und Klicken Sie auf „OK“, um die Einstellung zu übernehmen.

12.9.4 Seriell-Ethernet-Gateway einrichten

Das Seriell-Ethernet-Gateway ermöglicht es, aus dem lokalen Netzwerk des MoRoS UMTS PRO 2.0 oder von der Ferne aus serielle Endgeräte anzusprechen, die an der seriellen Schnittstelle des MoRoS UMTS PRO 2.0 angeschlossen sind. An einen konfigurierbaren Netzwerkport des MoRoS UMTS PRO 2.0 gesendete Daten werden an der seriellen Schnittstelle des MoRoS UMTS PRO 2.0 ausgegeben. Die serielle Schnittstelle kann auch zum Anschluss eines redundanten Kommunikationsgeräts benutzt werden. In diesem Fall ist die Schnittstelle nicht als Seriell-Ethernet-Gateway benutzbar.

Konfiguration mit Weboberfläche

Um das **Seriell-Ethernet-Gateway** einzurichten, aktivieren Sie im Menü „Server-Dienste“ auf der Seite „Seriell-Ethernet“ die Checkbox „Seriell-Ethernet-Gateway aktivieren“.

Die **Geschwindigkeit der seriellen Schnittstelle** stellen Sie im Eingabefeld „Geschwindigkeit (in Bit/s)“ ein.

Das **Datenformat der seriellen Schnittstelle** stellen Sie im Eingabefeld „Datenbits / Paritätsbits / Stopbits“ ein.

Die **Datenflusskontrolle** (RTS/CTS Handshake) stellen Sie im Eingabefeld „Flusskontrolle“ ein. Sollte das angeschlossene serielle Gerät die RTS/CTS-Leitungen nicht unterstützen, müssen Sie die Flusskontrolle deaktivieren.

Um die **Steuerleitungen** DCD und DTR zu verwenden, aktivieren Sie die Checkbox „Steuerleitungen benutzen“.

Damit die **Steuerleitungen nach dem Ende der Verbindung zurückgesetzt** werden, aktivieren Sie die Checkbox „Steuerleitungen nach Verbindungsende zurücksetzen“.

Damit die **TCP-Verbindung automatisch beendet** wird, **wenn kein Datentransfer** mehr stattfindet, stellen Sie im Eingabefeld „Timeout“ einen Wert in Sekunden ein. Findet so lange wie hier angegeben kein Datentransfer mehr statt, wird die TCP-Verbindung, die von einem Rechner zum Seriell-Ethernet-Gateway aufgebaut wurde, geschlossen. Damit die Verbindung niemals beendet wird, stellen Sie hier den Wert „0“ ein. Der Wert „0“ ist Standardeinstellung.

Den **Port**, unter dem das Seriell-Ethernet-Gateway eine TCP-Verbindung entgegennimmt, geben Sie im Eingabefeld „Port“ ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.9.5 Proxy-Server konfigurieren

Der MoRoS UMTS PRO 2.0 bietet einen Proxy-Server. Dieser dient **nicht** als Cache für häufig aufgerufene Internetseiten. Er dient zum Verzögern der Verbindungstimeouts bei langsam aufbauenden Wählverbindungen (z.B. via Modem) und zum Ausfiltern von unerwünschten URLs (z.B. www.xyz.xx).

Der Proxy unterstützt die Protokolle HTTP und HTTPS.

Konfiguration mit Weboberfläche

Um den **Proxy-Server des MoRoS UMTS PRO 2.0 einzuschalten**, aktivieren Sie im Menü „Server-Dienste“ auf der Seite „Proxy“ die Checkbox „Proxy-Server aktivieren“.

Stellen Sie im Eingabefeld „**Port des Proxy-Servers**“ den Port ein, unter dem Sie den Proxy-Server aus dem internen Netz unter der IP-Adresse des MoRoS UMTS PRO 2.0 erreichen wollen.

Um **Verbindungen nach einer bestimmten Zeit zu beenden, die nicht mehr aktiv scheinen,** können Sie im Eingabefeld „Timeout für inaktive Verbindungen“ die Zeitdauer anpassen.

Um eine **Überlastung des MoRoS UMTS PRO 2.0 zu vermeiden**, können Sie die Anzahl der Clients beschränken, die sich gleichzeitig mit dem MoRoS UMTS PRO 2.0 verbinden können. Geben Sie die maximale Anzahl gleichzeitig erlaubter Clients in das Eingabefeld „Maximale Anzahl an erlaubten Clients“ ein.

Um die **Verfügbarkeit des Proxys zu erhöhen**, können Sie eine minimale Anzahl von Proxy-Server-Prozessen festlegen. Geben Sie die gewünschte Anzahl von ständig auf dem MoRoS UMTS PRO 2.0 laufenden Proxy-Server-Prozessen im Eingabefeld „Minimale Anzahl an freien Proxy-Servern“ ein.

Um eine **Überlastung des MoRoS UMTS PRO 2.0 mit Proxy-Anfragen zu verhindern**, können Sie eine maximale Anzahl von Proxy-Server-Prozessen festlegen. Für jede Anfrage eines Clients wird ein einzelner Proxy-Server-Prozess auf dem MoRoS UMTS PRO 2.0 gestartet. Geben Sie dazu eine gewünschte maximale Anzahl von gleichzeitigen Proxy-Server-Prozessen in das Eingabefeld „Maximale Anzahl an freien Proxy-Servern“ ein. Werden mehr Anfragen empfangen als Proxy-Server verfügbar sind, werden die überzähligen Anfragen abgewiesen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.9.6 URL-Filter einrichten

Der Proxy des MoRoS UMTS PRO 2.0 kann mit Hilfe des URL-Filters die möglichen URLs beschränken, die aus dem internen Netz des MoRoS UMTS PRO 2.0 von Rechnern aufgerufen werden können. Damit werden nur noch Zugriffe auf URLs erlaubt, die in der Filterliste eingetragen sind, alle anderen URLs sind gesperrt. Um den Zugriff auf das Internet nur noch über den Proxy zuzulassen, ist außerdem die Aktivierung der Firewall erforderlich. Ohne die Firewall wäre der Zugriff auf beliebige URLs durch einfache Umgehung des Proxy möglich.

Auf den Clients (.z.B. einem Web-Browser auf einem PC), die über den Proxy Verbindungen aufbauen sollen, muss die IP-Adresse des Proxy eingestellt sein.

Konfiguration mit Weboberfläche

Um den **URL Filter einzuschalten**, aktivieren Sie im Menü „Server-Dienste“ auf der Seite „Proxy“ die Checkbox „Filter aktivieren“.

Um eine **zulässige URL einzutragen**, die aus dem internen Netz erreichbar sein soll, tragen Sie die gewünschte URL in die Eingabefelder „Erlaubte URLs“ ein.

Um eine **URL aus der Liste zu löschen**, löschen Sie den Text der URL aus der Liste.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.10 Systemkonfiguration

12.10.1 Systemmeldungen anzeigen

Der MoRoS UMTS PRO 2.0 zeigt Systemdaten wie Firmware-Version, Seriennummer, Hardware-Stand oder die Firmware-Prüfsumme zusammen mit kurzen Systemmeldungen über Ereignisse und Fehler im Menü „System“ auf der Seite „Systemdaten“ an. Für Analysezwecke können Sie sich die ausführlichen Meldungen des MoRoS UMTS PRO 2.0 auf der Weboberfläche ansehen.

Konfiguration mit Weboberfläche

Um einen die **ausführlichen Systemmeldungen über die Weboberfläche anzusehen**, klicken Sie auf den Link „Anzeigen des ausführlichen System Logs“.

12.10.2 Anzeigen der letzen Systemmeldungen

Der MoRoS UMTS PRO 2.0 zeigt kurze Systemmeldungen über Ereignisse und Fehler im Menü „System“ auf der Seite „Systemdaten“ an. Für Analysezwecke können Sie sich die letzten Meldungen des MoRoS UMTS PRO 2.0 anzeigen lassen.

Konfiguration mit Weboberfläche

Um die letzten **Systemmeldungen des MoRoS UMTS PRO 2.0 anzuzeigen**, klicken Sie auf den Link „Anzeigen der letzten Systemmeldungen“.

12.10.3 Uhrzeit und Zeitzone einstellen

Der MoRoS UMTS PRO 2.0 besitzt eine interne Uhr, um zeitabhängige Vorgänge steuern zu können. Diese Uhr müssen Sie einstellen, damit zeitabhängige Vorgänge auch zum gewünschten Zeitpunkt pünktlich ausgeführt werden und Systemmeldungen richtig datiert sind. Die Uhr des MoRoS UMTS PRO 2.0 kann automatisch über einen NTP-Server aus dem Internet aktualisiert werden. Bei jedem Verbindungsaufbau versucht der MoRoS UMTS PRO 2.0 die Uhrzeit vom festgelegten NTP Server zu synchronisieren. Die Zeitzone muss im Gegensatz zur Uhrzeit selbst manuell dem Standort des MoRoS UMTS PRO 2.0 angepasst werden.

Konfiguration mit Weboberfläche

Um die **Uhrzeit sowie das Datum einzustellen** geben Sie im Menü „System" auf der Seite „Zeit" die Werte für Tag, Monat, Jahr sowie Stunden und Minuten in die Eingabefelder „TT MM JJJJ hh mm" ein.

Stellen Sie **die Zeitzone des Einsatzorts des MoRoS UMTS PRO 2.0** ein, in dem Sie diese aus dem Dropdownmenü „Zeitzone" auswählen.

Um die **Uhrzeit sowie das Datum per NTP-Server zu synchronisieren**, aktivieren Sie die Checkbox „Uhrzeitsynchronisierung über" und geben Sie den Namen eines NTP-Servers oder dessen IP-Adresse in das Eingabefeld ein.

Um die **Uhrzeit sowie das Datum per NTP-Server täglich zu einem bestimmten Zeitpunkt zu synchronisieren**, aktivieren Sie die Checkbox „Zusätzlich jeden Tag um" und geben Sie die Uhrzeit für die tägliche Synchronisierung in das Eingabefeld ein.

Um die **Uhrzeit sowie das Datum per NTP-Server sofort zu einem synchronisieren**, aktivieren Sie die Checkbox „Uhrzeit sofort synchronisieren". Dann wird einmalig mit dem Speichern der Einstellungen versucht, eine Verbindung mit dem NTP-Server aufzubauen, um die Uhrzeit zu synchronisieren. Dies ermöglicht einen sofortigen Test der NTP-Server-Einstellungen.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK" klicken.

12.10.4 Zurücksetzen (Reset)

Sie können den MoRoS UMTS PRO 2.0 über die Weboberfläche oder mit dem Reset-Taster auf der Gerätevorderseite zurücksetzen. Sie können dabei das Gerät einfach neu starten oder alle Einstellungen auf Werkseinstellungen zurücksetzen. Mit dem Reset-Taster können Sie durch einmaliges, kurzes Drücken einen Software-Reset auslösen. Ein mindestens drei Sekunden dauerndes Drücken löst einen Hardware-Reset des MoRoS UMTS PRO 2.0 aus. Beide Male wird ein Neustart durchgeführt. Durch dreimaliges, kurzes Drücken innerhalb von zwei Sekunden laden Sie die Werkseinstellungen des MoRoS UMTS PRO 2.0.

Konfiguration mit Weboberfläche

Um den **MoRoS UMTS PRO 2.0 neu zu starten**, wählen Sie im Menü „System“ auf der Seite „Reset“ den Radiobutton „Neustart“ aus. Klicken Sie auf „OK“, um den Neustart durchzuführen.

Um den **MoRoS UMTS PRO 2.0 neu zu starten und gleichzeitig die Werkseinstellungen zu laden**, wählen Sie im Menü „System“ auf der Seite „Reset“ über den Radiobutton „Grundeinstellungen laden und neu starten“ aus. Klicken Sie anschließend auf „OK“, um den Neustart durchzuführen und den MoRoS UMTS PRO 2.0 auf die Werkseinstellungen zurückzusetzen.

Um einen **täglichen Neustart zu einem bestimmten Zeitpunkt zu konfigurieren**, aktivieren Sie die Checkbox „Täglicher Neustart um“ und geben Sie die Uhrzeit für den täglichen Neustart in das Eingabefeld ein.

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

12.10.5 Aktualisieren der Firmware

Sie können die Firmware des MoRoS UMTS PRO 2.0 aktualisieren. Die Firmware ist eine Zusammenstellung von Betriebsystem und Programmen, in der die Funktionen des MoRoS UMTS PRO 2.0 implementiert sind. Um die Firmware zu aktualisieren, benötigen Sie eine Datei mit einer neuen Firmware, die Sie auf Anfrage bei Ihrem Vertriebspartner oder bei INSYS MICROELECTRONICS erhalten. Bei umfangreicheren Aktualisierungen kann es sein, dass Sie zwei Dateien erhalten.

Hinweis



Funktionsverlust durch fehlerhaftes Update!

Durch einen Verbindungsabbruch während des Updates und einen darauffolgenden Neustart kann der MoRoS UMTS PRO 2.0 seine Funktion verlieren.

Solange die rote LED am MoRoS UMTS PRO 2.0 leuchtet dürfen Sie keinerlei Aktionen am Webinterface durchführen, die Spannungsversorgung nicht trennen und keinen Reset ausführen.

Starten Sie bei nach einem fehlgeschlagenen Update den MoRoS UMTS PRO 2.0 nicht neu und setzen Sie sich mit dem Support von INSYS MICROELECTRONICS in Verbindung.

Hinweis



Verlust der Erreichbarkeit!

Durch ein Firmwareupdate kann Ihr MoRoS UMTS PRO 2.0 seine bisherige Konfiguration verlieren. Dann ist Ihr MoRoS UMTS PRO 2.0 nur aus dem lokalen Netz über seine Standard IP-Adresse 192.168.1.1 erreichbar.

Führen Sie kritische Updates nur vor Ort durch und kontaktieren Sie den Support von INSYS MICROELECTRONICS

Vollständiges Update der Firmware des MoRoS UMTS PRO 2.0

Im Folgenden erfahren Sie, welche die Schritte Sie prinzipiell zum Update der Firmware eines MoRoS UMTS PRO 2.0 durchführen müssen.

- Sie haben Zugriff auf die Weboberfläche.
- Falls Sie über eine Wählverbindung auf die Weboberfläche des MoRoS UMTS PRO 2.0 zugreifen, muss die Verbindung lange genug bestehen, um die Uploads durchzuführen. Die Option „maximale Verbindungszeit“ sollte für das Update auf „0“ gesetzt werden, ebenso wie die „Idle Time“.
- Sie haben sichergestellt, dass die Stromversorgung des MoRoS UMTS PRO 2.0 während dem Updatevorgang nicht ausgeschaltet werden kann.
- Sie besitzen die Firmware-Datei mit dem Namen „system_<rev>“ sowie ggf. die Datei „data_<rev>. Die Datei(en) ist/sind auf dem PC auffindbar, von dem Sie das Update durchführen wollen.

1. ***Wechseln Sie im Menü „System“ auf die Seite „Update“.***

2. ***Klicken Sie auf Durchsuchen... und wählen Sie die Datei „system_<rev>“ aus.***

3. ***Klicken Sie auf OK , um mit dem Update zu beginnen.***

✓ Eine Seite mit einer Sicherheitsabfrage erscheint. Vergleichen Sie die angezeigte MD5-Prüfsumme mit der MD5-Prüfsumme der Datei (z.B. mit dem Programm md5sum.exe). Wenn sie übereinstimmen, wurde die Datei korrekt übertragen und Sie können mit der Aktualisierung fortfahren. Der Vorgang dauert je nach Firmwaregröße unterschiedlich lange, bis die Datei auf den MoRoS UMTS PRO 2.0 vollständig übertragen ist.

4. ***Bestätigen Sie die Abfrage mit Ja.***

✓ Der Updatevorgang startet. Der Browser wartet. Während des Updates leuchtet die Status-LED am MoRoS UMTS PRO 2.0 rot auf.

✓ Nach dem vollständigen Update wird eine Seite angezeigt, die Ihnen den erfolgreichen Updatevorgang bestätigt. Bis zum Erscheinen dieser Anzeige darf keinesfalls eine Aktion am Webinterface durchgeführt werden.

5. ***Wenn Sie auch die Datei „data_<rev>“ erhalten haben, gehen Sie mit der zweiten Datei „data_<rev>“ vor wie mit der ersten Datei, ohne vorher einen Neustart auszuführen. Wiederholen Sie die Schritte ab Schritt 1. Nach dem Hochladen erfolgt ein automatischer Neustart.***

6. ***Wenn Sie nur die Datei „system_<rev>“ erhalten haben, wechseln Sie im Menü „System“ auf die Seite „Reset“, wählen Sie „Neustart“ und klicken Sie auf OK.***

✓ Die neue Firmware ist nun aktiv.

12.10.6 Herunterladen der Konfigurationsdatei

Sie können die Konfiguration des MoRoS UMTS PRO 2.0 über die Weboberfläche herunterladen. Mit dieser Datei können Sie weitere, gleiche Geräte konfigurieren oder eine funktionierende Konfiguration sicher aufbewahren.

Konfiguration mit Weboberfläche

Um die **Konfiguration des MoRoS UMTS PRO 2.0 herunterzuladen**, klicken Sie im Menü „System“ auf der Seite „Download“ auf den blauen Pfeil. Sie werden dann vom Browser aufgefordert, die Datei abzuspeichern.

12.10.7 Hochladen der Konfigurationsdatei

Sie können eine zuvor herunter geladene Konfigurationsdatei auf den MoRoS UMTS PRO 2.0 hochladen, um die momentane Konfiguration des MoRoS UMTS PRO 2.0 durch die in der Datei enthaltenen Einstellungen zu ersetzen.

Hochladen der Konfigurationsdatei des MoRoS UMTS PRO 2.0

⇢ Sie besitzen eine Konfigurationsdatei für Ihre Version des MoRoS UMTS PRO 2.0.

1. ***Wechseln Sie im Webinterface des MoRoS UMTS PRO 2.0 unter „System“ auf die Seite „Update“.***

2. ***Klicken Sie auf Durchsuchen... und wählen Sie die Konfigurationsdatei (z.B. configuration.bin) aus.***

3. ***Klicken Sie auf OK , um mit dem Hochladen zu beginnen.***

✓ Eine Seite mit einer Sicherheitsabfrage erscheint.

4. ***Bestätigen Sie die Abfrage mit Ja.***

✓ Der Updatevorgang der Konfiguration startet.

✓ Nach dem vollständigen Hochladen der Konfiguration wird eine Seite angezeigt, die Ihnen den erfolgreichen Updatevorgang bestätigt.

5. ***Wechseln Sie im Menü „System“ auf die Seite „Reset“, wählen Sie „Neustart“ und klicken Sie auf OK.***

✓ Die neue Konfiguration ist nun aktiv.

12.10.8 Senden einzelner „Ping“-Pakete

Der MoRoS UMTS PRO 2.0 kann einzelne „Ping“-Pakete versenden. Damit lässt sich oft auf einfache Art und Weise testen, ob eine bestimmte Maschine im Netzwerk erreichbar ist. Der einzelne "Ping" kann optional periodisch wiederholt werden.

Konfiguration mit Weboberfläche

Um ein **einzelnes Ping-Paket zu versenden**, geben Sie die IP-Adresse, an die Sie das Ping-Paket senden wollen, im Menü „System“ auf der Seite „Piing“ in das Feld „IP-Adresse ein“ und klicken Sie auf „OK“. Die Antwort wird unten auf der Seite angezeigt.

Um das **Ping-Paket periodisch zu senden**, geben Sie in das Feld „Aktualisierung alle“ das Intervall in Sekunden an, in dem Sie das Ping-Paket an die konfigurierte IP-Adresse senden wollen. Wenn Sie hier „0“ eingeben, wird das Ping-Paket nur einmal gesendet

Speichern Sie Ihre Einstellungen, indem Sie auf „OK“ klicken.

13 Entsorgung

13.1 Rücknahme der Altgeräte

Gemäß den Vorschriften der WEEE ist die Rücknahme und Verwertung von INSYS-Altgeräten für unsere Kunden wie folgt geregelt:

Bitte senden Sie Ihre Altgeräte frachtfrei an folgende Adresse:

Frankenberg-Metalle
Gärtnersleite 8
96450 Coburg
Deutschland

Diese Vorschrift gilt für Geräte aus Lieferungen ab dem 13.08.2005.

14 Konformitätserklärung



Declaration of Conformity

Equipment: **UMTS - Router**

Type: **MoRoS UMTS 2.0 PRO**

Hereby the equipment is confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility 89/336/EEC and the Council Directive relating to Low Voltage 73/23/EEC as well as the Council Directive R&TTE 1999/5/EG.

The following company is responsible for this declaration:

INSYS Microelectronics GmbH
Waffnergasse 8
D-93047 Regensburg

For the evaluation of above mentioned Council Directives for Electromagnetic Compatibility, Low Voltage and R&TTE following standards were consulted:

DIN EN 55022: 2003-09 class B
DIN EN 61000-6-2:2002-08

ETSI EN 301 489-1:V.1.4.1
ETSI EN 301 489-7&-24:V.1.2.1
ETSI EN 301 511:V.9.0.2
ETSI EN 301 908-1&-2 V2.2.1

DIN EN 60950-1:2003-03

INSYS MICROELECTRONICS

INSYS MICROELECTRONICS GmbH
Waffnergasse 8
D-93047 Regensburg
Tel: 0941 - 560061
FAX: 0941 - 563471

Regensburg, 24.04.2009

Date / Place

Signature of responsible Person

15 Lizenzen

Die im MoRoS UMTS PRO 2.0 verwendeten Software -Technologien und Programme der Firmware sind zum Teil an die im Folgenden aufgeführten Lizenzen gebunden. Der Quellcode der an diese Lizenzen gebunden Teile der Firmware des MoRoS UMTS PRO 2.0 kann auf Anfrage von INSYS MICRO-LECTRONICS bezogen werden.

15.1 GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and

so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

15.2 GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming

the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.

- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

15.3 Sonstige Lizenzen

OpenVPN license:

Copyright (C) 2002-2005 OpenVPN Solutions LLC <info@openvpn.net>

OpenVPN is distributed under the GPL license version 2 (see below).

Special exception for linking OpenVPN with OpenSSL:

In addition, as a special exception, OpenVPN Solutions LLC gives permission to link the code of this program with the OpenSSL library (or with modified versions of OpenSSL that use the same license as OpenSSL), and distribute linked combinations including the two. You must obey the GNU General Public License in all respects for all of the code used other than OpenSSL. If you modify this file, you may extend this exception to your version of the file, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

LZO license:

LZO is Copyright (C) Markus F.X.J. Oberhumer, and is licensed under the GPL.

Special exception for linking OpenVPN with both OpenSSL and LZO:

Hereby I grant a special exception to the OpenVPN project (http://openvpn.net/) to link the LZO library with the OpenSSL library (http://www.openssl.org).

Markus F.X.J. Oberhumer

OpenSSL License:

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in

the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT,

INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

16 Internationale Sicherheitshinweise

Der folgende Sicherheitshinweis von Cinterion in Englisch gilt für die verwendete UMTS-Engine HC25. Auf jedes Gerät ist nach den amerikanischen Vorgaben der FCC ein Aufkleber mit dem Hinweis auf die „FCC ID“ angebracht.

16.1 Safety Precautions

The following safety precautions must be observed during all phases of the operation, usage, service or repair of any cellular terminal or mobile incorporating HC25. Manufacturers of the cellular terminal are advised to convey the following safety information to users and operating personnel and to incorporate these guidelines into all manuals supplied with the product. Failure to comply with these precautions violates safety standards of design, manufacture and intended use of the product. Cinterion assumes no liability for customer’s failure to comply with these precautions.

When in a hospital or other health care facility, observe the restrictions on the use of mobiles. Switch the cellular terminal or mobile off, if instructed to do so by the guidelines posted in sensitive areas. Medical equipment may be sensitive to RF energy.
The operation of cardiac pacemakers, other implanted medical equipment and hearing aids can be affected by interference from cellular terminals or mobiles placed close to the device. If in doubt about potential danger, contact the physician or the manufacturer of the device to verify that the equipment is properly shielded. Pacemaker patients are advised to keep their hand-held mobile away from the pacemaker, while it is on.

Switch off the cellular terminal or mobile before boarding an aircraft. Make sure it cannot be switched on inadvertently. The operation of wireless appliances in an aircraft is forbidden to prevent interference with communications systems. Failure to observe these instructions may lead to the suspension or denial of cellular services to the offender, legal action, or both.

Do not operate the cellular terminal or mobile in the presence of flammable gases or fumes. Switch off the cellular terminal when you are near petrol stations, fuel depots, chemical plants or where blasting operations are in progress. Operation of any electrical equipment in potentially explosive atmospheres can constitute a safety hazard.

Your cellular terminal or mobile receives and transmits radio frequency energy while switched on. Remember that interference can occur if it is used close to TV sets, radios, computers or inadequately shielded equipment. Follow any special regulations and always switch off the cellular terminal or mobile wherever forbidden, or when you suspect that it may cause interference or danger.

Road safety comes first! Do not use a hand-held cellular terminal or mobile when driving a vehicle, unless it is securely mounted in a holder for speakerphone operation. Before making a call with a hand-held terminal or mobile, park the vehicle.

Speakerphones must be installed by qualified personnel. Faulty installation or operation can constitute a safety hazard.

IMPORTANT!

Cellular terminals or mobiles operate using radio signals and cellular networks. Because of this, connection cannot be guaranteed at all times under all conditions. Therefore, you should never rely solely upon any wireless device for essential communications, for example emergency calls.

Remember, in order to make or receive calls, the cellular terminal or mobile must be switched on and in a service area with adequate cellular signal strength.

Some networks do not allow for emergency calls if certain network services or phone features are in use (e.g. lock functions, fixed dialing etc.). You may need to deactivate those features before you can make an emergency call. Some networks require that a valid SIM card be properly inserted in the cellular terminal or mobile.

17 Glossar

Hier werden die wichtigsten Begriffe und Abkürzungen aus dem Handbuch kurz beschrieben.

APN: Access Point Name, Rechnername der Mobilfunkteilnehmern des GPRS-Netzes Zugang zum Internet bietet.

AT-Befehl: Kommando an Geräte wie z.B. Modems, mit dem dieses Gerät eingestellt wird.

Broadcast: Datenpaket, das an alle Teilnehmer eines Netzwerks gesendet wird.

Caller ID: Die Rufnummer, die der Anrufer übermittelt und von dem angerufenen Gerät interpretiert werden kann.

Client: Gerät welches Dienste von einem anderen Gerät (Server) anfordert.

CLIP: Calling Line Identification Presentation ist ein Leistungsmerkmal für ankommende Rufe im analogen und ISDN Telefonnetz sowie bei Mobilfunk. Dem Empfänger wird die Caller-ID des Anrufers übermittelt.

CHAP: Challange Handshake Authentication Protocol, Ein Authentifizierungsprotokoll, das oft bei PPP-Verbindungen benutzt wird.

DHCP: Dynamic Host Configuration Protocol, DHCP-Server können DHCP-Clients auf deren Anfrage dynamisch eine IP-Adresse und andere Parameter übergeben.

Dial-In: MoRoS kann über eine Wählverbindung angerufen werden und eine Verbindung zum LAN herstellen.

Dial-Out: MoRoS kann über eine Wählverbindung anrufen, und z.B. eine Verbindung ins Internet herstellen.

DFÜ: Datenfernübertragung, Daten können zwischen Computern über weite Distanzen übertragen. Die Übertragung wird oft mit Modems und dem PPP-Protokoll realisiert.

DNS: Domain Name System, Dienst der für die Umsetzung von Domainnamen in IP-Adressen benutzt wird.

Domainname: Die Domain ist der Name einer Internetseite (z.B. insys-tec). Sie besteht aus dem Namen und einer Erweiterung (Top Level Domain, z.B. .de), (z.B. insys-tec.de).

EDGE: Enhanced Data Rates for GSM Evolution bezeichnet eine Technik zur Erhöhung der Datenrate in GSM-Mobilfunknetzen durch Einführung eines zusätzlichen Modulationsverfahrens. Mit EDGE werden GPRS zu E-GPRS (Enhanced GPRS) und HSCSD zu ECSD erweitert.

Firewall: Netzwerkregeln, die vor allem Datenpakete zu bestimmten Absendern oder Zielen blocken.

Gateway: Dies ist eine Maschine, die wie ein Router arbeitet. Im Gegensatz zum Router kann ein Gateway auch Datenpakete von unterschiedlichen Hardware-Netzwerken routen.

GPRS: General Packet Radio Service, Weiterentwicklung des ->GSM-Mobilfunknetzes um höhere Datenübertragungsraten erreichen zu können.

GSM: Global System for Mobile communications, Mobilfunknetz für Sprach- und Datenübertragung.

ICMP: Internet Control Message Protocol, Protokoll, das oftmals für die Steuerung eines Netzwerks benutzt wird. Das Programm „ping“ benutzt z.B. ICMP.

IP-Adresse: Internet Protokoll Adresse, die IP-Adresse eines Gerätes in einem Netzwerk unter der es erreicht werden kann. Sie besteht aus vier Byte und wird dezimal angegeben, (z.B. 192.168.1.1)

ISP: Internet Service Provider, dieser kann über eine Wählverbindung (z.B. mit analogen Modem oder ISDN-TA) angerufen werden. Der ISP sorgt dann dafür, dass man über diese Wählverbindung einen Zugang zum Internet erhält.

LAN: Lokal Area Network, ein Netzwerk aus Rechnern, die örtlich relativ nah beisammen sind.

MAC-Adresse: Media Access Control Address. Ein MAC ist ein Teil eines Ethernetinterfaces. Jedes Ethernetinterface hat eine weltweit einzigartige Nummer, die MAC-Adresse.

MSN: Multiple Subscribers Number. Geräte die an einem S0-Bus aktiv sind, benötigen eine Teilnehmerkennung in Form einer Endgerätenummer.

Netzmaske: Definiert eine logische Gruppierung von IP-Adressen in Netzwerkadresse und Geräteadressen.

Netzwerkadresse: Besteht aus der Überlappung von IP-Adresse und Netzmaske. Sie endet immer mit „.0“. Die Netzmaske (z.B. 255.255.255.0) wird binär über eine IP-Adresse (z.B. 192.168.1.1) gelegt, der noch „sichtbare“ Teil dieser Überlappung (Maskierung) ist die Netzwerkadresse (hier: 192.168.1.0).

Netzwerkregeln: sie entscheiden, wie die unterschiedlichen Datenpakete in einem Netzwerkgerät gehandhabt werden, sie können z.B. Datenpakete an oder von bestimmten Netzwerkteilnehmern gesperrt oder umgeleitet werden.

PAP: Password Authentication Protocol, ein Authentikationsprotokoll, das oft bei PPP-Verbindungen benutzt wird.

Port: (1) Buchse am Switch, an der Ethernet-Geräte angeschlossen werden.
(2) Bestandteil eines Sockets bei Datenverbindungen

Portforwarding: Netzwerkregeln, die Datenpakete von bestimmten Absendern zu besonderen Empfängern eines Netzwerkes umleiten.

PPP: Point to Point Protocol, ein Protokoll, das zwei Maschinen über eine serielle Leitung so miteinander verbindet, dass sie TCP/IP-Pakete austauschen können.

Router: Dies ist eine Maschine, die in einem Netzwerk dafür sorgt, dass die bei ihm eintreffenden Daten eines Protokolls zum vorgesehenen Zielnetz bzw. Subnetz weitergeleitet werden.

SCN: Service Center Number, Rufnummer des Rechners, der Kurzmitteilungen (->SMS) über das GSM-Netz entgegennimmt und zu den Empfängern weiterleitet.

Server: Gerät, das anderen Geräten (Client) Dienste zur Verfügung stellt, z.B. Webserver.

SMS: Short Message Service, Kurzmitteilungen können über das Mobilfunknetz GSM versendet werden

Socket: Datenverbindungen, die per ->TCP oder ->UDP zustande kommen, arbeiten zur Addressierung mit Sockets. Ein Socket besteht aus einer IP-Adresse und einem Port (vgl. Anschrift: Straßenname und Hausnummer)

Switch: Ein Gerät, das mehrere Maschinen mit Ethernet verbinden kann. Im Gegensatz zu einem Hub „denkt“ ein Switch mit, d.h. er kann sich die MAC-Adressen merken, die an einem Port angeschlossen sind und lenkt den Verkehr effizienter zu den einzelnen Ports.

TCP: Transmission Control Protocol, ein Transportprotokoll, um den Datenaustausch zwischen Netzwerkgeräten zu ermöglichen. Es arbeitet „verbindungsorientiert“, d.h. die Datenübertragung ist gesichert.

UDP: User Datagram Protocol, Transportprotokoll, um Datenaustausch zwischen Netzwerkgeräten zu ermöglichen. Es arbeitet „verbindungslos“, d.h. die Datenübertragung ist ungesichert.

UMTS: Universal Mobile Telecommunications System steht für den Mobilfunkstandard der dritten Generation (3G), mit dem deutlich höhere Datenübertragungsraten (384 kbit/s bis 7,2 Mbit/s) als mit dem Mobilfunkstandard der zweiten Generation (2G), dem GSM-Standard (9,6 kbit/s bis 220 kbit/s) möglich sind.

URL: “Uniform Resource Locator”, sie bezeichnet die Adresse, unter der ein Service im Webbrowser gefunden werden kann. In diesem Handbuch wird als URL meist die IP-Adresse des MoRoS eingegeben.

VPN: Virtual Private Network, über bestehende unsichere Netzwerke werden logische Verbindungen (sog. Tunnel) aufgebaut. Die Endpunkte dieser Verbindungen („Tunnelenden“) und die Geräte dahinter können als eigenes, logisches Netzwerk betrachtet werden. Mit Verschlüsselung der Datenübertragung über die Tunnel und die vorherige gegenseitige Authentifizierung der Teilnehmer an diesem logischen Netzwerk kann ein sehr hoher Grad an Abhör- und Manipulationssicherheit erreicht werden.

WAN: Wide Area Network, ein Netzwerk aus Rechnern, die örtlich weit auseinander liegen.

18 Tabellen & Abbildungen

18.1 Tabellenverzeichnis

18.2 Abbildungsverzeichnis

19 Stichwortverzeichnis